Fall 2014

A stochastic multi-criteria assessment of security of transportation assets

Michelle Sophie Dojutrek
Purdue University

Graduate School Form 30
(Revised 08/14)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Michelle Sophie Dojutrek

Entitled

A Stochastic Multi-Criteria Assessment of Security of Transportation Assets

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

Dr. Samuel Labi

Dr. J. Eric Dietz

Dr. Fred L. Mannering

Dr. Kumares C. Sinha

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification/Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Dr. Samuel Labi

Approved by Major Professor(s): _____

Approved by: Dr. Dulcy M. Abraham 12/10/2014

Head of the Department Graduate Program Date

A STOCHASTIC MULTI-CRITERIA ASSESSMENT OF SECURITY OF TRANSPORTATION ASSETS

A Dissertation
Submitted to the Faculty
of
Purdue University
by
Michelle Sophie Dojutrek

In Partial Fulfillment of the
Requirements for the Degree
of
Doctor of Philosophy

December 2014
Purdue University
West Lafayette, Indiana

To my family.

ACKNOWLEDGEMENTS

There are many people I would like to acknowledge who have mentored, guided, and educated me during my Ph.D. at Purdue University. First, I would like to express the utmost appreciation and respect for my advisor, Dr. Samuel Labi whose patience, knowledge, and dedication have been very important to my development as a scholar and expert. Thank you for taking the time to teach me the skills necessary to develop my research techniques, and I appreciate all of the time you spent discussing the finer details of the transportation field. My deepest gratitude also goes to my committee members, Dr. Kumares Sinha , Dr. Fred Mannering, and Dr. Eric Dietz for their help and support along the way. I am honored have been mentored by such distinguished members of the transportation and security fields.

My sincere appreciation also goes to the many people at Purdue who have shared their knowledge to help me complete this research. I cannot thank enough Ms. Dorothy Jane Miller and Ms. Jenny Ricksy in the School of Civil Engineering for their support throughout the years. Great thanks to all my Purdue friends as well, both in and outside the department, who made my Ph.D. studies more stimulating. Our numerous dinners and outings allowed for a wonderful balance between school and recreation.

Most of all, I owe all that I have achieved to my family for always supporting and encouraging me to continue on my journey. I am thankful for their endless love, prayers,

and guidance. I would also like to thank my friends who have supported me from near and afar, particularly Stephanie Everett, Kristi Selden, Alyssa Block, Marisa De Nicolo, and Jessica Cheng. Without your candor and encouragement, I could not have gotten this far. Finally, I thank Purdue University for this amazing opportunity to learn about the world from a mathematical and quantitative view.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

KEY TERMS

Security	-	A function of threat likelihood, asset resilience and damage consequences.
Factor	-	Plays an integral role in quantifying security of an asset.
Measure	-	Quantifies how much the factor contributes to asset security.
Attribute	-	Level of the measure rated on a scale to define the overall amount that the measure contributes to the factor.
SR	-	Security Rating
Asset	-	Specific transportation infrastructure (roadways, bridges, tunnels, pipeline, airports, guardrails, etc.).
Threat	-	Any unexpected natural, unintentional man-made or intentional man-made event that causes damage or disruption.
Threat Likelihood	-	The probability of a threat occurring that effects the asset.
Resilience	-	The ability of the asset to withstand and recover from the threat.
Consequence	-	The effects of the failure of an asset and its associated costs and damages.
NBI	-	National Bridge Inventory
ESR	-	Existing Security Rating
ISR	-	Increase in Security Rating
FSR	-	Final Security Rating
GIS	-	Geographic Information System
ADT	-	Average Daily Travel
NOAA	-	National Oceanic and Atmospheric Administration
EDMC	-	Elemental Decomposition and Multi-criteria

ABSTRACT

Dojutrek, Michelle Sophie. Ph.D., Purdue University, December 2014. A Stochastic Multi-Criteria Assessment of Security of Transportation Assets. Major Professor: Dr. Samuel Labi.

Transportation project evaluation and prioritization use traditional performance measures including travel time, safety, user costs, economic efficiency, and environmental quality. The project impacts in terms of enhancing the infrastructure resilience or mitigating the consequences of infrastructure damage in the event of disaster occurrence are rarely considered in project evaluation. This dissertation presents a methodology to address this issue so that in evaluating and prioritizing investments, infrastructure with low security can receive the attention they deserve. Secondly, the methodology can be used for evaluating and prioritizing candidate investments dedicated specifically to security enhancement. In defining security as a function of threat likelihood, asset resilience and damage consequences, this dissertation uses security-related considerations in investment prioritization thus adding further robustness in traditional evaluations. As this leads to an increase in the number of performance criteria in the evaluation, the dissertation adopts a multiple-criteria analysis approach. The methodology quantifies the overall security level for an infrastructure in terms of the threats it faces, its resilience to damage, and the consequences in the event of the infrastructure damage. The dissertation demonstrates that it is feasible to develop a security-related measure that can be used as a performance criterion in the evaluation of

general transportation projects or projects dedicated specifically towards security improvement. Through a case study, the dissertation applies the methodology by measuring the risk (and hence, security) of each for bridge infrastructure in Indiana. The method was also fuzzified and a Monte Carlo simulation was run to account for unknown data and uncertainty. On the basis of the multiple types of impacts including risk impacts such as the increase in security due to each candidate investment, this dissertation shows how to prioritize security investments across the multiple infrastructure assets using multiple-criteria analysis.

CHAPTER 1: INTRODUCTION

1.1. Importance of Transportation Infrastructure

National transportation systems are vast interconnected networks of diverse modes and due to its diversity and size; these infrastructure systems play a major role in the economy and national security of nations (Steffey, 2008). The transportation industry comprises many modes of travel (air, rail, vehicle, waterway, pipeline) and involves over nine million jobs that enable a monumental amount of passengers and goods to move throughout the world annually (Polzin 2012; DHS, 2011; BLS, 2011). Activities in the transportation sector make up 12% of the gross domestic economy and most businesses rely on a functioning transportation system to move their products. In the United States, the marine transportation system, including ports, waterways, and vessels, handles more than $900 billion in international commerce every year (Lundquist, 2011). Freight revenue on railroads in 2010 was $56.3 billion (AAR, 2012). Air transportation revenue in the U.S. totaled $134.7 billion in 2011, 6.8% higher than the previous record set in 2008 (Herbst, 2012).

There are about 600,000 bridges in the overall U.S. network with approximately 1,000 identified as “critical” due to possible casualties, economic disruption, or other consequences if they are rendered dysfunctional for any reason (AASHTO, 2003). The losses due to a critical bridge or tunnel could exceed $10 billion. The U.S. transportation

system includes 337 highway tunnels and 211 transit tunnels, many of which are located under bodies of water and may have limited alternative routes due to geographic constraints (AASHTO, 2003). There are 8,606,003 lane-miles of pavement in the United States (FHWAa, 2014). Railway has a total of 139,118 miles of infrastructure within the U.S. (FHWA, 2011). Shipping and ports are vital elements in the economic and military activities of most countries in the world due to their extensive size, open accessibility, and metropolitan location that ensure a free flow of trade, but present great challenges to effective monitoring and control of traffic (Steffey, 2008).

The abundance of infrastructure networks has led to their criticality in performing the functions of everyday life as well as their interconnectedness with other infrastructure networks, industries, and workforces that rely upon them (Barker et al., 2013). Because of its diversity and size, a national transportation system is vital to a country's economy and national security. Without the transportation industry, thousands of jobs directly or indirectly connected to this industry, would be lost, and products and goods would not be mobile within and outside of the country. Malevolent attacks, natural disasters, man-made accidents, or common failures can have significant widespread impacts when they lead to the failure of network components (Barker et al., 2013). If one part of the system is impaired, delays and stagnant goods would hinder companies' profits, cause user delays, and disrupt everyday life. Intermodal transportation would also be affected if one mode is unable to complete its part of transporting a good or passengers. Transportation plays a major role in a country's economy and therefore should be made as resilient as possible to failures or damage to enable necessary mobility.

1.2. Threats to Transportation Infrastructure

Disasters can result in millions and even billions of dollars worth of damage not only to the physical infrastructure but also in terms of the economic and social consequences resulting from impaired functionality of the infrastructure. For example, Hurricane Sandy, which hit the U.S. eastern coast in 2012, caused about $50 billion in damages, and the 2011 tsunami in Japan caused about $308 billion in damage (Porter, 2013; Ridgwell, 2011). Also, events such as the Paramount Boulevard Bridge accident in California cost $40 million in damages and repair and the Leo Frigo Memorial Bridge Pier failure in Wisconsin cost $20 million in investigation and repair costs (Tata, 2012; Phelps, 2013). The occurrence and magnitude of natural or man-made disasters cannot be predicted with absolute certainty; however, if civil infrastructure systems can be made to better withstand the potential damage resulting from these disasters, the consequences and costs of repair may be reduced.

Similar to all civil infrastructure systems, transportation assets encounter end-of-life situations when they face intended or unintended agents that cause their destruction (Labi, 2014). Unintended termination can be caused by the failure of the asset itself due to factors including design flaws, fatigue, advanced deterioration, and other internal causes; or due to external agents such as overloading, accidents, or natural events. Intended end-of-life events include deliberate retirement due to structural or functional obsolescence. Also, transportation infrastructure make attractive targets of intentional harmful attacks because of their visibility, accessibility, and capacity to carry large numbers of commuters in a relatively confined space (Steffey, 2008). Maritime and

surface transportation systems are vulnerable to attacks by terrorists who seek to attract publicity, and any successful attack can inflict high numbers of civilian casualties and cause political and economic disruption (Steffey, 2008). Transportation assets are widely distributed and most routes have multiple entry points and open accessibility which precludes 100% protection of these assets (Steffey, 2008). This in turn necessitates that a certain degree of risk of damage or destruction is always attached to these transportation assets.

1.3. Assessing Risks and Protecting Transportation Infrastructure

Security-related system engineering is defined as the protection of physical infrastructure components and logical structures and processes from threats and vulnerabilities (Garcia, 2001). As Polzin (2012) stated, transportation requires security for numerous reasons including: it is a critical element of the economy; it is a gathering place for groups of people; it has symbolic and emotional importance; it provides a delivery means for people and products; it includes institutions with licensing and enforcement responsibilities. As a National Cooperative Highway Research Program panel stated, “the source of the threat was only one issue -- the loss of an asset has the same consequence whatever the cause of the loss” (Cambridge and Parker, 2011). Security concerns play a large role in how transportation facilities and services are provided (Polzin, 2012). Malicious individuals regularly attempt to disrupt the operations of modern transport; worse still, terrorists seek to reap political dividends by attacking transportation infrastructure and seeking its destruction (Flynn, 2000). The consequences,

which are numerous, include: casualty impact (the potential for loss or serious injury to human life); business continuity (the extent to which loss or serious damage to the asset would impair the ability of the agency to continue to operate); economic impact (the extent to which loss or serious damage to the asset would affect the viability of business going forward); replacement cost (the capital investment required to replace the asset); and replacement downtime (the length of time before the asset can be returned to service) (Frazier, 2009).

Existing normal methodologies for assessing and managing risks to transportation infrastructure provide a valuable conceptual structure and practical tools for allocating resources in cost-effective ways to improve public safety (Steffey, 2008). The U.S.'s National Infrastructure Protection Plan was updated in 2009 to build a safer, more secure and resilient country by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate or exploit elements of the nation's critical infrastructure and key resources (Fisher and Norman, 2010). The Transportation Security Administration (TSA) pledged to follow a systems-based risk-management approach that incorporates three main elements: threat, vulnerability (including criticality), and consequence (Steffey, 2008). Publicly Available Specification 55 Part 2 (PAS 55-2) in the UK states that risk management is fundamental for proactive asset management and that its purpose is to understand the cause, effect and likelihood of adverse events occurring in order to manage these risks to an acceptable level (Hooper et al., 2009). The International Infrastructure Management Manual (IIMM) is a guidance document focused on the experiences of Australia, New Zealand, UK, South Africa and the U.S. (INGENIUM, 2006). IIMM recommends that core asset management should

identify critical assets and events and should apply risk management techniques to these assets (Hooper et al., 2009). The Department of Homeland Security (DHS) Enhanced Critical Infrastructure Protection (ECIP) program has a goal of providing owners and operators with information to help them make better-informed risk management decisions; DHS collects data during ECIP visits to support risk reduction investment parameters and processes, identify gaps that require additional programming, activities and functions to mitigate, and understand and inform the national risk picture through detailed analysis (Fisher and Norman, 2010).

There are a few general steps that are required to help reduce unintentional natural or man-made termination of transportation infrastructure. The first is to measure the threat likelihood posed by external forces to the asset itself. If the threats are at all predictable based on historical data such as earthquake occurrence or tendency to flood, these measurable threat probabilities can help determine if an asset is located in a high threat area. Second, the threat likelihood can be monitored over time to see if patterns arise so the asset can be improved to increase its physical resistance or resilience before the threat strikes. Third, the benefits of any implemented improvements must be assessed in terms of their effectiveness in reducing the possible consequences in the event of a threat occurrence. The fourth step involves communicating the gathered information to serve as evidence for securing the needed funding for security investments. What is missing from these steps is a way to quantify security to be able to tell which assets are at the greatest overall risk. As such, a better case could be made to help improve the security of the transportation infrastructure.

Uncertainty must be considered when working with security factors. Hazards are highly non-deterministic. For example, the magnitude of earthquakes or the number of accidents cannot be predicted at 100% accuracy. The failure to consider uncertainty could lead to assets being unprepared for the potential range of hazards that could impair the asset and ultimately, widen consequences to the community and the economy. It is possible to account for uncertainty using historical data trends and predictive models to provide a range of likelihood scenarios for hazards that could potentially harm the asset.

In any given jurisdiction, there typically exists a wide range of threat types to transportation infrastructure; however, if such threats to each asset can be identified, and if the expected reduction in the asset damage due to security-enhancing investments can be predicted, the reduction in the disaster consequences can be estimated. When infrastructure is made resilient through security investments, the consequences of end-of-life events can be reduced and the infrastructure itself can play a role in mitigating or recovering from the overall damage resulting from the event.

1.4. Problem Statement

At present, the funding allocation processes for transportation infrastructure at most agencies utilize performance measures that include the expected change in asset condition or remaining life, economic efficiency, energy use, land use, air quality, connectivity, and so on (Sinha and Labi, 2007). However, the impacts of competing investments on asset security are rarely considered in a direct manner. Thus, for assets that are located in an area of high threat likelihood, their respective candidate investments

could help reduce the potential for infrastructure damage (and the consequent adverse impacts on the community). Current evaluation processes do not account for such beneficial impacts of the investments. As such, it is reasonable to argue that a performance measure that quantifies the security benefits (reduction of infrastructure damage risk due to external threats) should be considered in transportation investment evaluation and also in the prioritization of funds dedicated specifically to security.

Current funding allocation processes for transportation infrastructure rely on key parameters. For example, asset performance measures (age, condition, etc.), area performance measures (e.g. air quality), maintenance cycles, and budgets are studied to determine which specific assets receive funds for asset reconstruction or rehabilitation. For assets located in high threat areas (e.g., an area with high potential for earthquakes or landslides), current performance measures would most likely not reflect these situations and cannot suffice in a comprehensive evaluation of such project evaluations. As such, a performance measure quantifying security must be considered in the multi-criteria decision making process as another important key measure for investment prioritization. This would further align with the goals set by the Homeland Security Transportation Systems Sector: prevent and deter acts of terrorism against the transportation system; enhance the all-hazards preparedness and resilience of the global transportation system; improve the effective use of resources for transportation security; improve sector situational awareness, understanding, and collaboration (DHS, 2011).

There are five key steps to risk management that should be considered to develop evidence for security investments: measure the threat likelihood posed by external or intentional threats to the asset; monitor the threat likelihood over time; assess the

effectiveness of actions intended to reduce consequences; communicate this information to the general public and legislators; and provide evidence for appropriate resources. On the basis of these steps, a methodology should be developed and thereby make it feasible to consider security as one of the performance measures for general investment evaluation or to establish a priority list of assets for security investment.

The first step is to measure the threat likelihood posed by forces external to the asset. If historical data such as earthquake occurrence or flooding tendency are available, then these threat probabilities can be calculated to identify the areas of high threat likelihood. The second step states that the threat likelihood can be monitored over time to identify the optimal time of intervention. The third step states that the effectiveness of asset improvements can be assessed in terms of the extent to which they can reduce the damage or other adverse consequences if the threat does occur. The fourth step involves communicating the gathered information to serve as support material for requesting funding purposely for investments geared toward securing the infrastructure from damage. With these steps and a required security metric, a case for improving transportation infrastructure in terms of security, can be made or strengthened.

1.5. Objectives/Scope

There are four main objectives of this dissertation. The first is to develop a methodology to quantify security for each asset for all relevant threats to that specific asset which incorporates the five steps of risk management. The second objective is to incorporate dynamic concepts into the methodology to capture uncertainty. The third

objective is to apply the methodology to carry out prioritization of security investments. The fourth objective is to apply the methodology to investment evaluation on the basis of multiple criteria. The overall framework can be used for varying kinds of infrastructure (marine, power, other transportation modes, real estate), however, the case study is described specifically in the context of highway infrastructure.

The overarching goal of this dissertation is to support strategic resource allocation decisions at the asset level by providing meaningful measures of security risk that lend themselves to quantitative benefit-cost analysis (McGill et al., 2007). Since primary responsibility for management of incidents involving transportation normally rests with State and local authorities and the private sector, which own and operate the majority of the nation's transportation resources (Emergency Support Function #1 Annex Policies Section-Transportation Annex), this methodology would be useful in deciding which assets should receive funds to improve their security.

1.6. Organization of the Dissertation

This dissertation is organized into eight chapters. Chapter 1 presents the role of transportation in the economy and provides the rationale for protecting transportation infrastructure. The chapter also presents the dissertation's problem statement, objectives, and scope. Chapter 2 presents a literature review of the current risk assessment methodologies and discusses the general security variables and how the methods define the terminology. Chapter 3 describes the proposed security metric that was developed in this dissertation to address the limitations of traditional methods. Chapters 4 and 5 use the

developed method to assess security at the asset level and network level. Chapter 6 introduces dynamic concepts into the method developed in the dissertation and provides case studies. Chapter 7 discusses how to incorporate the security metric into investment decision making and project evaluation, and Chapter 8 summarizes and concludes the dissertation and provides directions for future research on this topic.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

Risk assessment involves the concepts of threat, vulnerability, and consequence information. Risk management, on the other hand, involves deciding which protective measures to take based on an agreed upon risk reduction strategy (Moteff, 2005). The security industry has been slow to use measurable factors in reducing risk because of difficulties in establishing security-related metrics (SAIC & PB Consult, 2009). Due to the difficult nature of quantifying key components of threat, vulnerability, and consequence, transportation security risk analysis generally employ qualitative methods in making judgments about the magnitudes of various risk situations (Steffey, 2008). Many in the security industry believe that qualitative analysis is sufficient to address the protection of lower value assets. Typically, a qualitative assessment assigns relative values to specific assets based on factors such as the criticality of loss or replacement costs. The threats against assets are also given a relative value based on their probability of occurrence. The result is a risk equation that computes risk as both a function of impact and likelihood of incidence. The goal of a security design strategy should be the logical and incremental “buy down” of security risk, in order to provide acceptable levels of protection for transportation agency assets and operations on a continuing basis (SAIC & PB Consult, 2009).

2.1.1. Terminology

The terminology used when describing security related factors include the terms defined in Table 2.1. which are found in the literature.

Table 2.1. Security Terminology

	Term	Definition	Consistent with:
Asset-related Terms	Target	Transportation asset that has value to the owner or users	SAIC & PB Consult, 2009
	Resilience	The ability of the asset to withstand the threat	Flynn and Burke, 2011
Threat-related Terms	Threat	An unexpected natural, unintentional man-made or intentional man-made event that causes damage or disruption	SAIC & PB Consult, 2009
	Threat Likelihood	The probability of a threat effecting the asset	Ayyub et al., 2007
Consequence-related Terms	Consequence	The loss of an asset and its associated costs and damages	SAIC & PB Consult, 2009

2.2. Threat

Threat likelihood is defined as the probability that an external or internal threat will occur (Labi, 2014). This definition involves the specific threat type and characteristics of the infrastructure such as location and orientation. Threats to civil infrastructure are in the form of unintended damage and intended damage, with the added categories of internal damage and external damage. For example, external unintended threats could be a sudden event like an earthquake, or a gradual event such as those seen during a freeze-thaw. Internal unintentional threats may be design flaws or aging of the

infrastructure itself. Intentional man-made threats take on the form of terrorist attacks and vandalism, while other man-made threats consist of overloading and collisions. Figure 2.1 below from Labi (2014) describes the different variations threats to civil infrastructure can take.

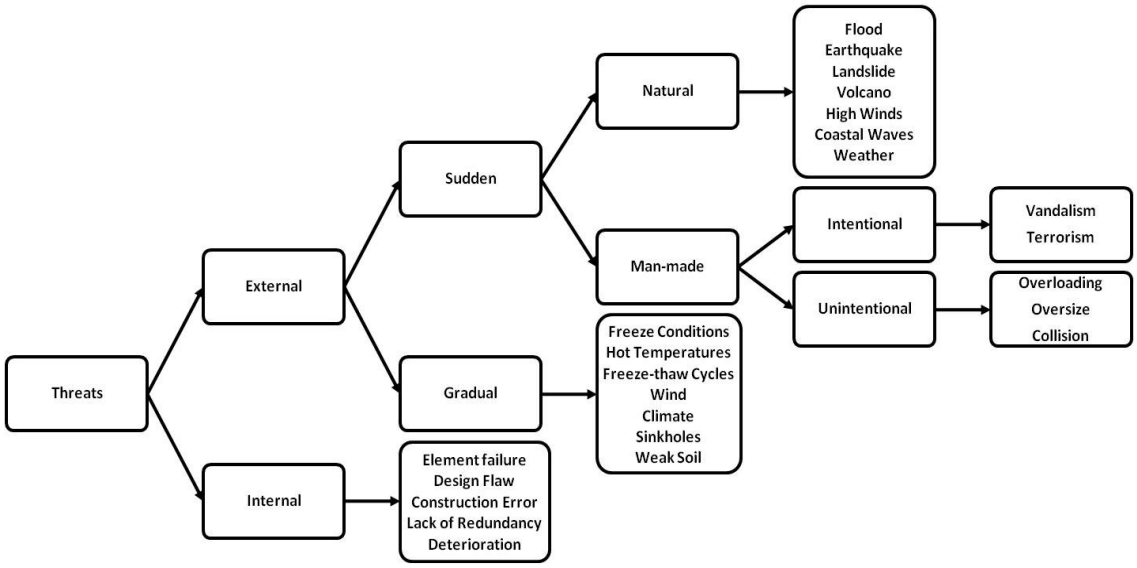


Figure 2.1. Possible Threats to Civil Infrastructure

The USDOT and FHWA organized threats to a transportation asset management program into three groups: asset specific, program specific, and management specific (FHWA, 2012). Examples of asset specific threats, both internal and external, include:

- Premature asset failures caused by faulty construction or materials;
- Chance failures caused by unpredicted events such as barges striking bridges or truck fires weakening beams;
- Abrupt failures caused by climatic or seismic events such as flooding, landslides or seismic activity, or;
- “Creeping failure” caused by gradual degradation spurred by traffic, environmental factors, corrosion and climate.

Program specific threats include:

- Wear-out failures caused by inadequate maintenance programs;
- Decision failures caused by inaccurate data or models;
- Resource failures caused by reductions in appropriations or increases in prices;
- Operational failures caused by process breakdowns, or;
- Demand failures caused by unanticipated vehicle loadings.

Management specific threats include those decisions made by agencies or owners of transportation infrastructure including:

- The failure to manage physical assets for the long term as official policy;
- Legislative mandates such as "worst first" that could detract from sound asset management;
- Substantial reductions in asset management funding, or;
- Internal bureaucratic resistance to asset management that can be addressed only by senior leadership.

Threat assessment identifies and evaluates potential treats on the basis of factors such as capabilities, intentions, and past occurrences (Steffey, 2008). Quantifying and assessing risk involves the calculation and comparison of probabilities, but most expressions involve compound measures that consider both the probability of harm and its severity (Melnick and Everitt, 2008). ASCE SEI determined that the estimation probability of failure involves the evaluation of: (i) the probability of the occurrence of a particular type of hazard or combination; (ii) the maximum intensity of the hazards that the system is exposed to within its service life; (iii) the probability that the system will exhibit a particular level of damage/local failure/collapse should the hazard take place.

Threat likelihood data can be derived from past figures detailing the frequency of occurrence or simulation of the event using theoretical resources.

2.3. System Resilience

Resilience can be defined as the ability to manage risks and bounce back quickly from damage (Flynn and Burke, 2011). A study by Barker et al. (2013) focuses on two dimensions of resilience over time, vulnerability and recoverability, for the development of a resilience-based component importance measure (CIM) for system analysis. Resilience can also be defined as a function of infrastructure age, condition, material type, design type, and other physical characteristics of which help the infrastructure recover after a disruption by a threat (Labi, 2014). The New Mexico Environmental Finance Center stated that an asset "may be highly likely to fail if it is old, has a long history of failure, has a known failure record in other locations, and has a poor condition rating; and an asset may be much less likely to fail if it is newer, is highly reliable, has little to no history of failure and has a good to excellent condition rating" (EFC, 2006).The Infrastructure Security Partnership (2011) noted that a resilient infrastructure sector would "prepare for, prevent, protect against, respond or mitigate any anticipated or unexpected significant threat or event" and "rapidly recover and reconstitute critical assets, operations, and services with minimum damage and disruption" (Barker et al., 2013). The Resilient Systems Working Group (RSWG) of the International Council on Systems Engineering (INCOSE) was established to enhance systems resilience so that the recovery from disasters could be enhanced. A working definition for resilience developed

by the RSWG is as follows: “the capability of a system with specific characteristics before, during, and after a disruption to absorb the disruption, recover to an acceptable level of performance, and sustain that level for an acceptable period of time” (INCOSE, 2012). Gunderson and Pritchard (2002) defined engineering resilience as “the speed of return of the engineering system to the steady state following a perturbation, which implies a focus on the efficiency of the function”. In general, however, no common definition or quantitative approach has been adopted for resilience (Henry and Ramirez-Marquez, 2012).

Resilience for the purposes of this dissertation will incorporate the concept of vulnerability and its assessment. However, the transportation sector generally does not build infrastructure for the “maximum of maximums” or extreme cases. For example, the resources needed to make infrastructure withstand an asteroid collision is not feasible, therefore the term resilience captures the infrastructure’s ability to withstand threats of types and intensities that can be reasonably expected, given its location and characteristics. General steps of vulnerability assessment include: identifying critical assets to be assessed, assessing vulnerabilities and criticality, assessing consequences, identifying countermeasures, and estimating the costs of these countermeasures (Venna and Fricker, 2009). The importance of infrastructure vulnerability analysis has been accentuated by the increasing realization that greater attention needs to be paid to infrastructure monitoring in order to prevent unexpected and catastrophic failure since infrastructure vulnerability is further exacerbated by inadequate condition (Kumar et al., 2011). The U.S. House Transportation and Infrastructure Committee quantifies about 70,000 bridges as structurally deficient out of the total 600,000 bridges on the National

Highway System (USCG, 2010). Patidar et al. (2008) argued that geo-hazard vulnerability should be duly considered in prioritization processes. If a bridge or other infrastructure is structurally deficient or functionally obsolete, the vulnerability to geo-hazards is higher (Kumar et al., 2011).

Informed decisions regarding vulnerability assessment and emergency response are essential for secure and safe operation of highway assets (Venna and Fricker, 2009). The National Cooperative Highway Research Program (NCHRP) for the American Association of State Highway and Transportation Officials (AASHTO) created the Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection to accompany the Guide to Updating Highway Emergency Response Plans for Terrorist Incidents (SAIC, 2002). The vulnerability assessment methods in the guide are adaptable to any State DOT, regardless of their critical infrastructure protection plan and help with assessing the vulnerability of highway transportation assets.

A vulnerability index (protective measures index) was developed by Fisher and Norman (2010) to compare differing protective measures. A resilience index was also developed to assess a site's resilience and consists of three primary components: robustness, resourcefulness, and recovery. Third, a criticality index that determines the importance of a facility and includes economic, human, governance, and mass evacuation impacts was developed. These indices were developed for the Enhanced Critical Infrastructure Protection initiative that DHS protective security advisers implement across the nation at critical facilities (Fisher and Norman, 2010).

2.4. Exposure and Consequences

Consequence is a function of the effect on the community (injuries, lives lost) and the natural and built-up environment (ecological resources, man-made facilities) if the infrastructure is damaged due to a threat as well as the infrastructure's exposure to the threat (Labi, 2014). Figure 2.2 provides a visual of the effect of consequences to civil infrastructure on its surrounding environment (Labi et al, 2011). Consequence assessment involves the nature of the threat and the impact of the loss of the asset (Steffey, 2008). The consequence associated with an event occurring can be described in multiple ways, and assessing these consequences can be in the form of the dollar value of resources damaged or destroyed and cost of repair, replacement, or substitution (Venna and Fricker, 2009). Consequences associated with asset failure may include loss of life and property, loss of infrastructure needed to support economic activity, military deployment, or the ability to respond effectively to other emergencies (SAIC, 2002). ASCE SEI determined that the evaluation of consequence of failure requires the assessment of: i) the cost of maintenance/ repair/ replacement of the system; ii) user cost and safety; iii) the failure impact on local and regional economic activity, and; iv) the political ramification to the affected communities.

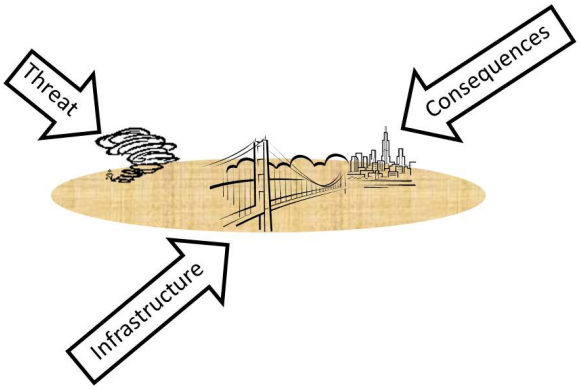


Figure 2.2. Impacts on the Surrounding Environment due to Infrastructure Threats

The New Mexico Environmental Finance Center states: "in terms of the consequence of failure, it is important to consider all of the possible costs of failure including: cost of repair, social cost associated with the loss of the asset, repair/replacement costs related to collateral damage caused by the failure, legal costs related to additional damage caused by the failure, environmental costs created by the failure, and any other associated costs or asset losses" (EFC, 2006). Variables to assess consequences include (Venna and Fricker, 2009):

- Fatalities/Casualties – Dead and injured as a result of the event.
- Mission Downtime/Degradation – Time the facility is unable to continue operation at full capacity or at all.
- Economic Impact – Direct economic impact on the facility to repair or replace (not including lawsuits, etc.).
- Downstream Effects – The extent of the downstream impact on the transportation system.

"Judgment of the relative importance of assets proceeds on the basis of critical factors such as casualty risk, potential effects on government continuity and emergency response, the military importance of the asset, economic impact, and the availability of alternative resources to perform an asset's primary function" (Steffey, 2008). Assessing

criticality requires an examination of the likelihood of failure and the consequence of failure; the assets that have the greatest likelihood of failure and the greatest consequences associated with the failure will be the assets that are the most critical (EFC, 2006). The IIMM defines critical assets as those where the consequences of an event occurring are high, but are not always associated with a high probability of occurrence (Hooper et al., 2009). Core asset management necessitates the identification of critical assets. To determine criticality, two pertinent questions must be answered, (i) how likely the asset is to fail and (ii) what is the consequence if the asset does fail. The data available to assist in determining whether an asset will fail includes: asset age, condition assessment, failure history, historical knowledge, experiences with that type of asset in general, and knowledge regarding how that type of asset is likely to fail (EFC, 2006). The importance of criticality allows a system to manage its risk, aids in determining where to spend operation and maintenance dollars, and helps facilitate capital expenditures (EFC, 2006).

2.5. General Assessment of Risk of Infrastructure Damage

Threat, vulnerability, and consequence information are important in risk assessment while risk management involves deciding which protective measures to take based on an agreed upon risk reduction strategy (Moteff, 2005). Risk assessment has been defined as an overall process of risk identification, risk analysis, and risk evaluation by British Standard 31100 (BSI, 2011). The American Society of Civil Engineers (ASCE) Structural Engineering Institute (SEI) Technical Council on Life-cycle

Performance, Safety, Reliability, and Risk of Structural Systems Questionnaire outlines risk assessment as involving the quantification of risk defined as the product of failure probability and failure consequence probability for systems subjected to different hazards or combination of hazards. Risk assessment can be strategic at the network level, tactical at the asset type/group level or operational at the asset level (Hooper et al., 2009).

ASCE SEI also describes risk management as the decision-making process and actions taken to preempt and mitigate risk. Due to the difficulties in quantifying key components of risk assessment, analyses of transportation security risk typically employ qualitative methods in making judgments about the relative magnitudes of various risk scenarios (Steffey, 2008). Quantitative risk assessment is an important growing component of the larger field of risk assessment that includes priority setting and management of risk (Melnick and Everitt, 2008). Risk information is useful for emergency managers and first responders when creating evacuation or emergency response routes. With quantitative risk information, legislative officials would have the ability to identify areas of concert and allocate resources appropriately.

The Oxford English Dictionary (online) defines risk as "(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility." Risk is typically a multidimensional concept which is often expressed as the Cartesian product in the context of risk analysis for critical infrastructure (McGill et al., 2008) as shown in Equation 1. The definitions of risk vary, but in relation to infrastructure asset management, a risk definition should involve the combination of probability and consequence of any uncertain event (Hooper et al., 2009).

$$Risk = threat \bullet vulnerability \bullet consequence \quad (1)$$

Where *threat* is a set of adverse initiating events, *consequence* is the spectrum of losses that can be felt by the victims following their occurrence, and *vulnerability* is a set of system of target weaknesses that can be exploited by an adversary to achieve a given degree of loss.

A threat-based risk analysis approach begins with a predefined set of threat scenarios based on assumed adversary capabilities justified by intelligence and proceeds through the analysis of vulnerability and consequence constrained by the definition and scope of these threats (McGill et al., 2007). This approach is suitable for studying hazards that are well understood and whose rate of occurrence can be reasonably predicted from historical data. Asset-driven risk analysis assesses the consequences and probability of adversary attack for an exhaustive set of plausible threat scenarios without regard to their probability of occurrence, and then overlays threat likelihood based on the relative attractiveness of alternative threat scenarios to obtain an estimate of total risk (McGill et al., 2007). This approach brings all plausible threat scenarios to attention in an attempt to defeat the potential for surprise attack without regard to adversary intent.

The model described above is the currently accepted model of risk assessment, but there is room for improvement. The concept of asset resilience should be incorporated into the security quantification equation as a separate factor focusing on the characteristics of the asset. Probability of threat would capture the probability of a threat happening, while the concept of resilience would capture the asset specific

characteristics. Furthermore, uncertainty should be incorporated into the risk analysis to capture the range of possible consequences affecting a specific asset.

2.6. Specific Methodologies for Assessing Risk of Infrastructure Damage

At the asset level, strategic and tactical risk assessment is useful to identify critical assets that require risk assessment. When not all assets require risk assessment in a larger group of assets, strategic risk assessment is acceptable with tactical risk assessment where needed (Hooper et al., 2009). In the transportation sector, some of the commonly used methodologies include: Analytical Risk Methodology (ARM), Maritime Sector Risk Analysis Methodology (MSRAM), DHS Transit Risk Analysis Methodology (DHS-TRAM), CARVER, Sandia National Labs Risk Assessment Methodologies (RAM), and the Homeland Security Comprehensive Assessment Model (HLS-CAM). The plethora of methodologies has resulted partly from a lack of precision in the formulation of data collection elements and a less-than-rigorous quality review of process by the government and security industry; what works in the closed and highly regulated aviation sector from the standpoint of SVA would not transfer well to the open and ubiquitous public transit system (SAIC & PB Consult, 2009). A security vulnerability assessment would be more beneficial if conducted by a trained team of security professionals using an industry-accepted methodology rather than a self-assessment questionnaire or checklist.

2.6.1. National Infrastructure Protection Plan Risk Assessment

The National Infrastructure Protection Plan proposed a methodology to assess the risk to critical infrastructure defined as assets, systems, and networks deemed vital to the USA, whose incapacitation or destruction would have a debilitating effect on security, economy, public health, or safety (DHS, 2010). The risk assessment methodology has three main components: vulnerability, resilience, and criticality which help determine comprehensive, cost-effective, and coordinated programming to manage the resiliencies and vulnerabilities of critical infrastructure. Risk is defined as a function of threat, vulnerability, and consequence of the failure of a critical infrastructure facility. In this case, resilience is included in the consequence factor. The risk is illustrated using a bowtie representation (Figure 2.3) originally developed to assess chemical processes which combines events and consequence trees, and allows characterization of pre- and post-event elements (Philley, 2006). It is used to explain the relationship between vulnerability, resilience, and criticality.

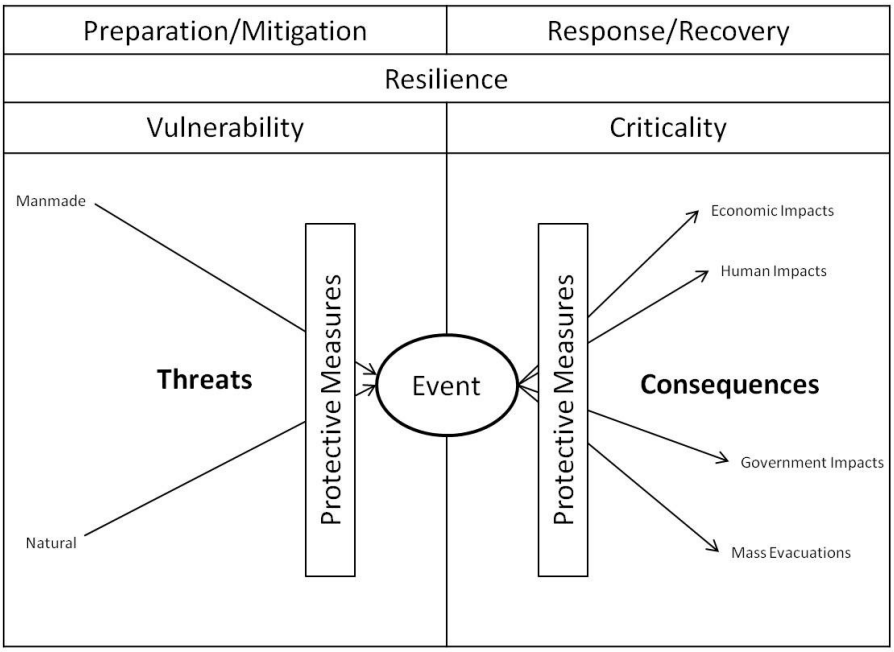


Figure 2.3. Risk Bowtie (Philley, 2006)

In this model, vulnerability is the capability of the system to resist a threat which is directly linked to the protective measures in place and the state of the system when the threat occurs. Resilience is the capability of the system to avoid or reduce the consequences set in motion when a threat event is successful and is also linked to the state of the system. Finally, criticality represents the severity of the consequences to the facility, the system, and the community. With these definitions, the bowtie scheme enables the entire spectrum of risk to be represented for a specific facility and/or allows explanation of the different types of measures that can be used to manage this risk and to reinforce the system (Fisher and Norman, 2010).

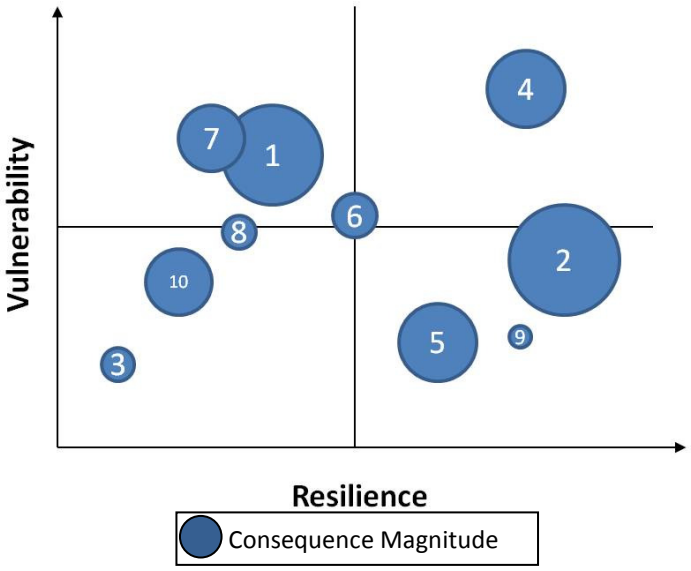


Figure 2.4. Risk Matrix (Fisher and Norman, 2010)

The indices used in the methodology can be plotted as seen in Figure 2.4. to help decision-makers visualize which facilities have the highest relative risk. The vulnerability index is on the y-axis, the resilience index is on the x-axis, and the criticality index is represented by a circle (the larger the circle, the greater the consequence). Facilities with the highest relative risk are identified by high vulnerability, low resilience and high criticality. Low relative risk is represented by facilities with low vulnerability, high resilience, and low criticality. The example in Figure 2.4. indicates that facilities 1 and 7 should be brought to the attention of the agency that oversees their security. These facilities have the lowest resilience, highest vulnerability, and highest criticality.

2.6.2. AASHTO Vulnerability Assessment Method

The AASHTO Vulnerability Assessment method is a guide for agencies to develop a vulnerability assessment method based on AASHTO's outlined steps. The

methodology focuses on subjectively assigning values to factors associated with asset criticality and vulnerability. Asset criticality and vulnerability scores are transformed into X and Y coordinates respectively and plotted to determine asset importance. Examples of criticality factors range from deter/defend factors to consequence to general public factors (SAIC, 2002). Assets are then prioritized based on the subjective values assigned to each factor in Table 2.1 using Equation 2 below.

Table 2.2. Critical Asset Scoring (SAIC, 2002)

Critical Asset	**Critical Asset Factor**					**Total Score (x)**
Asset 1	Factor 1	Factor 2	Factor 3	Factor 4	Factor *m*	
Asset 2						
Asset 3						
Asset *n*						

$$Criticality\ Coordinate\ (X) = \left(\frac{x}{C_{max}}\right) \cdot 100 \quad (2)$$

Where x is the total criticality score for asset n; and C_{max} is the highest criticality score attainable.

Vulnerability in the AASHTO vulnerability assessment is broken into three factors: Visibility and Attendance, Access to the Asset, and Site Specific Hazards (SAIC, 2002). Each factor is broken into two sub-factors and again given subjective values on a scale of one to five. The sub-factors for each main factor are then multiplied together and those results are added together as seen in Equation 3 below.

$$Vulnerability\ Factor\ (y) = (A \cdot B) + (C \cdot D) + (E \cdot F) \quad (3)$$

Where A and B are sub-factors of Factor 1; C and D are sub-factors of Factor 2; and E and F are sub-factors of Factor 3.

A vulnerability coordinate is derived for each asset using Table 2.2 and Equation 4 below.

Table 2.3.Vulnerability Factor Scoring (SAIC, 2002)

Critical Asset	**Vulnerability Factor**						**Total Score (y)**
	(A * B) + (C * D) + (E * F)						
Subjective Value Range	1-5	1-5	1-5	1-5	1-5	1-5	
Asset 1							
Asset 2							
Asset 3							
Asset *n*							

$$Vulnerability\ Coordinate\ (Y) = \left(\frac{y}{V_{max}}\right) \cdot 100 \quad (4)$$

Where V_{max} is the highest attainable vulnerability score; and y is the vulnerability total score for asset n.

The assets are then plotted in the following coordinate system (Figure 2.5) and assets falling in Quadrant 1 of the graph are the assets of importance.

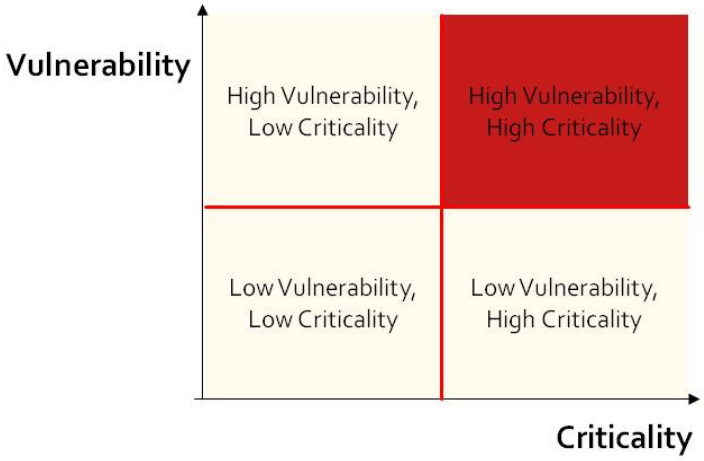


Figure 2.5. AASHTO Vulnerability Assessment

Consequence assessment is to be assumed from the graph in Figure 1 based on the X and Y coordinates and their factors and sub-factors. The method goes further by listing possible countermeasures broken down into countermeasure functions of deter, detect, and defend to be considered for the assets that fall in quadrant 1. Again, choosing

countermeasures is a subjective process based on the countermeasure functions and decision-maker. Finally, the countermeasures listed are given high, medium, and low rankings based on operational costs to help in the selection process.

A vulnerability assessment for rural transportation networks was assessed by Nachtmann et al. 2007 who selected AASHTO's vulnerability guide as the most robust vulnerability assessment tool. An alternative vulnerability assessment was also developed that included the Analytic Hierarchy Process to provide importance rankings within AASHTO's framework as a modification. The AASHTO methodology for risk management is quite subjective and uses surveys to obtain data (Venna and Fricker, 2009). Additionally, vulnerability and criticality are the only major factors included in the method to determine asset security importance, while concepts such as resilience are not (Dojutrek et al, 2014). Further, the method defines vulnerability and criticality as separate entities, but the concepts are quite similar. If an asset is vulnerable, then it has high criticality and vice versa.

2.6.3. TMSARM Vulnerability Self Assessment Tool

The TMSARM Vulnerability Self Assessment Tool developed by the Transportation Security Agency (TSA) is a self-assessment tool that guides a user through a series of security-related questions to develop a comprehensive security baseline of a transportation asset and assists users in the development of a comprehensive security plan. The user is then prompted to assess the baseline security system effectiveness in response to specific threat scenarios. The effectiveness is then reassessed

based upon the addition of countermeasures in response to conditions of heightened threat. The method was originally developed for maritime vulnerability and risk assessment for the U.S. Coast Guard's regulatory efforts promulgated the Maritime Transportation Security Act (MTSA) of 2002 (Coast Guard, 2003). A requirement of the MTSA is that any facility or vessel that may be involved in a transportation security incident should conduct a vulnerability assessment and submit a security plan to the U.S. Coast Guard. The MTSA defines a transportation security incident as "a security incident that results in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area" (Federal Register, 2002). The tool is available to company security officers, vessel security officers, and facility security officers. This tool has restricted access and is available only to certain companies and agencies (Venna and Fricker, 2009).

2.6.4. CARVER+Shock Vulnerability Assessment Tool

The CARVER method was originally developed as an offensive target analysis tool that was used by the Army Special Forces for mission planning based on a commander's objectives (Clark and Philpott, 2011). The method allowed the U.S. military to identify areas within critical or military infrastructure that are vulnerable to an attack. CARVER identifies six vulnerability factors (FDA, 2009):

- Criticality - measure of public health and economic impacts of an attack
- Accessibility - ability to physically access and egress from target
- Recuperability - ability of system to recover from an attack

- Vulnerability - ease of accomplishing attack
- Effect - amount of direct loss from an attack as measured by loss in production
- Recognizability - ease of identifying target

The factors are subjectively assigned a value on the scale of 0 to 10 (NIICIE, 2007). The overall vulnerability score of a single target is the sum of the scores assigned to the seven criteria and can be compared to rank the vulnerability of the different targets relative to each other. The targets with the highest total rating have the highest potential vulnerability and should be considered for countermeasures (FDA, 2009). It accounts for target components of the target system and is applicable to features outside of transportation. This method was the standard security vulnerability assessment tool for many years before it was further developed into the CARVER+Shock method. The CARVER+Shock method added an additional factor of "Shock" to the factors. Shock incorporates the combined health, economic, and psychological impacts of an attack on the target system (FDA, 2009). Psychological impact is influenced by a large number of deaths if the target has historical, cultural, religious, or other symbolic significance and if victims are members of a sensitive subpopulation such as children (FDA, 2009).

Federal agencies, such as the Food Safety and Inspection Service (FSIS) and the Food and Drug Administration (FDA), have utilized the CARVER+Shock method to evaluate the potential vulnerabilities of farm-to-table supply chains of various food items. This method is useful when assessing the potential vulnerabilities of individual processing facilities (FDA, 2009). This methodology is popular as local governments seek to leverage simple analysis tools to derive security-related information. It provides a "quick and dirty" means to rank potential targets based on vulnerability. However,

McGill and Ayyub (2007) pointed out that its additive and inherently non-probabilistic nature does not produce results that can support security risk assessment.

2.6.5. Maritime Security Risk Analysis Model

The Maritime Security Risk Analysis Model (MSRAM) is a risk analysis tool employed by the U.S. Coast Guard. Similar to other methods, MSRAM assesses risk in terms of threat, vulnerability, and consequences. As a tool, MSRAM enables Federal Maritime Security Coordinators and Area Maritime Security Committees to perform detailed scenario risk assessments on all maritime critical infrastructure (DHSa, 2010). The model is used to inform strategic and tactical risk decision-making. The methodology is designed to capture the security risk facing various targets and assets that span multiple sectors. MSRAM is a scenario-based tool that evaluates threat, vulnerability, and consequences and considers mitigating options. This method facilitates operational planning and resource allocation, prioritization of sector assets, and a risk-based evaluation of port security grant proposals. Expanding the capabilities of MSRAM is an ongoing priority for the maritime mode (DHSa, 2010).

2.6.6. TCM Risk Assessment Method

The TMC Risk Assessment Methodology (TCM RAM) is a combination from three different sources, the Systematic Assessment of Facility Risk (SAFR), a separate methodology developed by the DHS Office of Domestic Preparedness toolkit, and ideas from AASHTO's Guide (SAIC, 2005). The steps in this method include: asset

identification, threat assessment, consequence assessment, vulnerability assessment, and countermeasure development. It evaluates risk using the following equation:

$$RR = TA \cdot T \cdot C \cdot (1 - LD) \cdot (1 - LS) \quad (5)$$

Where *RR* (Relative Risk) is a function of the overall threat to the asset or facility, *T*; the attractiveness of a particular target to a given adversary, *TA*; the potential consequences of a successful attack on a target, *C*; the ability to deter an adversary from attempting an attack, *LD* (expressed in terms of the inability to deter, or *1-LD*); and the effectiveness of the system to prevent an attack should one be attempted, *LS* (expressed in terms of system ineffectiveness, or *1-LS*).

Calculating the relative risk to one asset has limited value since it only indicates the risk to that asset relative to the highest and lowest possible *RR* (Venna and Fricker, 2009). The TMC RAM is a theoretically good model, but requires a lot of expert effort to quantify the value of subjective criteria which could input inconsistency and variance into the model. This method evaluates vulnerability and criticality in terms of relative risk and target attractiveness (Venna and Fricker, 2009).

2.6.7. CAPTA

The Costing Asset Protection for Transportation Agencies (CAPTA) method identifies security-related countermeasures for assets on the basis of the extent of potential losses (SAIC & PB Consult, 2009). CAPTA uses a consequence-based methodology that supports capital budgeting and resource allocation. The method establishes a consequence threshold for planning and resource allocation purposes rather

than focusing on assets, specific hazards, or threats, simplifying the risk management process. The main purpose of the method is to reduce risks to a level manageable by operating agencies based on their available budget and resources. Consequence thresholds are established subjectively for the risk factors that include the potentially-exposed population, property loss, and mission disruption. This method is mainly a decision-informing tool for capital budgeting, not necessarily an asset specific assessment tool for prioritizing assets (SAIC & PB Consult, 2009). It also focuses attention on significant, relevant assets, but eliminates those assets or asset classes whose loss of use would not exceed consequence thresholds, regardless of the hazard or threat from further consideration (SAIC & PB Consult, 2009).

2.6.8. Critical Asset and Portfolio Risk Analysis (CAPRA)

The critical asset and portfolio risk analysis (CAPRA) method was developed to consider both natural and human-caused hazards (Ayyub et al., 2007). The formula resembles a traditional model based on the notional product of consequence, vulnerability, and threat. The framework is as follows:

Scenario Identification→Consequence & Criticality Assessment→Security Vulnerability Assessment →Hazard Likelihood Assessment→ Benefit/Cost Analysis→ Risk Informed Decisions

Consequence and criticality assessment estimates the losses associated with each hazard scenario as a function of intensity. Equation 6 illustrates the consequence and criticality portion of CAPRA:

$$L_x = F_{\varepsilon|h} \cdot \left(1 - E_{M,\varepsilon}\right) \cdot L_{MC,h} \cdot (1 - E_R) \quad (6)$$

Where L_x is the loss as a function of hazard intensity attributed to hazard scenario x; $F_{\varepsilon|h}$ is the fragility of the target element ε due to hazard type h as a function of hazard intensity; E_M measures the resistance of the asset's mission to loss as a function of element damage; $L_{MC,h}$ is the maximum credible loss associated with hazard h; and E_R measures the effectiveness of response and recovery capabilities.

Vulnerability is taken as the probability of adversary success as a function of hazard intensity for a specific attack profile as seen in Equation 7:

$$P_{S,y} = \left(1 - E_{S,y}\right) \cdot P_K \cdot Q \quad (7)$$

Where $P_{S,y}$ is the probability of adversary success as a function of hazard intensity for a specified attach profile y; $E_{S,y}$ is the security system effectiveness with respect to the characteristics of attack profile y; P_K is the probability that the adversary will successfully execute its attack on the target given failure of the security system; and Q is the probability distribution for hazard intensity imparted on the target ($P_S = Q$ for natural hazards).

Hazard likelihood was defined as the product of the estimated annual rate of occurrence for a given hazard type, and for deliberate human-caused hazard. Equation 8 below outlines the relationships.

$$\lambda_y = A_{P,y} A_{S,x} A_{A,h} \lambda_{0,h} \quad (8)$$

Where λ_y is the annual rate of occurrence associated with a given attack profile y; $A_{P,y}$ is the relative attractiveness of attack profile y; $A_{S,x}$ is the relative attractiveness of hazard

scenario x, $A_{A,h}$ is the relative attractiveness of the asset with respect to hazard type h; and $\lambda_{0,h}$ is a baseline annual rate of occurrence.

The risk assessment portion is the combination of rate of attack, probability of adversary success given attack, and the loss given adversary success:

$$R_y = \int_0^{\infty}\{F_{\varepsilon|q}(1-E_{M,\varepsilon})L_{MC,h}(1-E_R)(1-E_{S,y})\cdot QA_{P,y}A_{S,x}A_{A,h}.\lambda_{0,h}\}\,dq \quad (9)$$

Where R_y is the annual risk associated with an attack profile y, hazard scenario x, and hazard type h; $L_{MC,h}$ is the maximum credible loss; $\lambda_{0,h}$ is the baseline annual rate of hazard occurrence.

$$R_h = L_{MC,h}V_h\lambda_{A,h} \quad (10)$$

Where R_h is the total hazard risk across all hazard scenarios and profiles for a given hazard type; $\lambda_{A,h} = A_{A,h}\lambda_{0,h}$ is the annual rate of occurrence for a given hazard affecting the asset; and V_h is the overall vulnerability as:

$$V_h = \sum_{x\epsilon X_h} A_{S,x}\left(\sum_{y\epsilon Y_x} A_{P,y}\left[\int_0^{\infty}\{F_{\varepsilon|h}(1-E_{M,\varepsilon})\cdot(1-E_R)\cdot(1-E_{S,y})Q\}dq\right]\right) \quad (11)$$

Where the summations are taken over all hazard scenarios X_h and corresponding attack profiles Y_x for a given hazard type h. Vulnerability can be interpreted as the degree of maximum credible loss following a hazard event that captures both the inherent physical and security weaknesses associated with different system statistics of an asset and its key elements (Ayyub et al., 2007).

2.6.9. Risk Filtering, Ranking, and Management Method

The Risk Filtering, Ranking, and Management (RFRM) method builds on hierarchical holographic modeling (Haimes et al., 2002) to identify risks then filters and

ranks the many sources of risks, enabling decision-makers to focus on the most critical. Hierarchical holographic modeling (HHM) is a comprehensive framework for identifying real and perceived sources of risk (Leung et al., 2004). Prioritized risks are evaluated in the risk management phase of this method and later reviewed in order to make future improvements to the system (Leung et al., 2004). The phases of the method are listed below and most rely on interview or survey techniques to gain the necessary data to run each scenario.

- Phase 1: Scenario identification through hierarchical holographic modeling
- Phase 2: Scenario filtering based on scope, temporal domain, and level of decision making
- Phase 3: Bi-criteria filtering and ranking
- Phase 4: Multicriteria evaluation
- Phase 5: Quantitative ranking
- Phase 6: Risk management
- Phase 7: Safeguarding against missing critical items

2.6.10. Summary of Assessment Methods

The methods described above mainly rely on the traditional risk equation which includes the threat, vulnerability, and consequence factors. Each method defines the terms in slightly different words and uses various measures to determine the levels of each. For example, AASHTO uses criticality and vulnerability as separate variables, but it could be argued that vulnerability is a function of criticality. Additionally, many of the methods described above rely heavily on the use of subjective data and complex data

collection to perform their analysis. Further, most methods did not look specifically at asset physical characteristics (e.g., age, material, design type). It is important to realize that the physical infrastructure can play a role in decreasing consequences by withstanding threats acting upon it. Finally, the methods described do not consider dynamic features throughout their frameworks and rarely mention capturing uncertainty.

2.7. Incorporating Analytical Techniques into Risk Assessment

A study done by Xia et al. (2004) developed a framework for risk assessment that includes static and dynamic infrastructure characteristics in the event of a terrorist attack. The risk score of a highway component is defined as a linear combination of three indices:

$$R = (\propto A + \beta B) \cdot \frac{C}{100} \tag{12}$$

Where R is the risk score of highway network component; A is the static characteristic index; B is the dynamic characteristic index; C is the attack potential index; α is the weight of the static characteristic index; and β is the weight of the dynamic characteristic index.

The static characteristics (Index A) include: structural stability, number of alternatives, and response resources of highway components. The dynamic characteristics (Index B) include: dynamic traffic flow information such as volume, speed, occupancy, vehicle classification, and queue length as well as weather details and work zone activities. The potential of a terrorism attempt (Index C) is estimated in terms of

functional significance and symbolic importance of a highway component (Xia et al, 2004).

The score of Index A is calculated as:

$$A = aW_{A1} + bW_{A2} + cW_{A3} + dW_{A4} \quad (13)$$

The score of Index B is calculated as:

$$B = eW_{B1} + fW_{B2} + gW_{B3} + hW_{B4} + iW_{B5} \quad (14)$$

The score of Index C is calculated as:

$$C = jW_{C1} + kW_{C2} \quad (15)$$

Where *W*'s are the weights predetermined with the help of experts; and *a, b, c, d, e, f, g, h, i, j, k* are characteristics pertaining to each index.

The Blue Ribbon Panel Approach to risk management first prioritizes bridge assets then completes a risk assessment (AASHTO, 2003). The risk assessment calculates risk as follows:

$$R = O \cdot V \cdot I \quad (16)$$

Where *R* is the risk to the facility; *O* is the occurrence or likelihood that terrorists will attack the asset (includes target attractiveness, level of security, access to the site, publicity if attacked, and the number of prior threats); *V* is the vulnerability or likely damage resulting from various terrorist threats (includes expected damage, outcome of the event, expected casualties, and loss of use, all features of the facility itself); and *I* is the importance or indication of consequences to the region or nation if the facility is destroyed.

The formula for *R* expresses the interaction among the three factors, where dominant factors magnify risk, while negligible factors diminish it (AASHTO, 2003).

Different formulas fail to account for their interactive effects, such as models that add factors (Venna and Fricker, 2009).

A method developed by Ray (2007) focuses on a single bridge asset and the risk associated with each of its many individual structural components. Within this study, risk is described as the relative potential for a terrorist attack against a specific component of the asset and the associated consequence from the attack. Factors used in the risk analysis include the component's importance to overall structural stability, location and accessibility to terrorists, and resistance to a specific threat. Results include a rank-ordered list of the components most at risk to an attack, which allows prioritization and optimization of the mitigation design for the bridge asset. The risk equation for a single bridge, for each of its *j* components exposed to threat *i,* is as follows:

$$R = \sum\left[I_j \sum\{O_{ij} V_{ij}\}\right] \tag{17}$$

Where *j* is the individual bridge component; *i* is the threat; O_{ij} is the measure of the probability of a threat *i* occurring against component *j*; V_{ij} is the vulnerability of component *j* given the occurrence of threat *i*; and I_j is the importance of an individual component *j* to the bridge.

Each factor is further broken down into weights and attribute factors which sum to a number between zero and one.

$$I_j = \sum[wf_k a_k]SR \tag{18}$$

$$O_{ij} = \sum[wf_k a_k] \tag{19}$$

$$V_{ij} = \sum[wf_k a_k] \tag{20}$$

Where wf_k is the weighting factor applied to the attribute a_k; a_k is the attribute or specific unity-based criteria of varied importance that sum together to define each factor; *SR* is the

span ratio for the bridge (ratio of the span length of the part component *j* is attached and the main bridge span).

2.7.1. Fuzzy Logic and Risk

Fuzzy logic was used in a study by McGill and Ayyub (2007) to approximate the true functional relationship between the effectiveness of six security system capabilities (access control, personnel barriers, vehicle barriers, surveillance systems, guard force, and reaction force with heavy weapons) and probability of adversary success. The goal of the model is to provide a system based on approximate reasoning that produces an estimate for the probability of adversary success based on the subjective evaluation of several or more defensive criteria. $Pr(S|A_i)$ is the probability of adversary success (S) given the occurrence of initiation event A_i and the complementary event $Pr(\bar{S}|A_i)$ as the security system effectiveness (McGill and Ayyub, 2008). Each defensive criterion (six security system capabilities) can take on a linguistic value of "Low," "Medium," or "High" defined on a constructed scale for effectiveness with membership functions. The Consequent Pr(S|A) may take on linguistic values such as "Likely," "Certain," or "Even Chance." There is the possibility that each defensive criterion may require its own set of linguistic phrases for effectiveness, for example if one criterion was based on a constructed scale and another on a crisp scale such as time (McGill and Ayyub, 2008). A user (security expert) can subjectively assign a value to each premise of criterion on a scale of 0-10 or an alternate scale for a given facility of asset and attack type once the fuzzy inference rules are defined.

Another study by Yazdani et al., (2012) uses Fuzzy TOPSIS as a fuzzy multi-criteria decision making technique to determine the weights of each criterion and the importance of alternatives with respect to criteria for risk analysis. This framework extends the Risk Analysis and Management for Critical Asset Protection (RAMCAP) method by introducing new parameters ("detectability" and "reaction against event") to assess the effects on risk value. "Detectability" is the potential and capability for identification and elimination of the weakness, and "reaction against event" is the capability of an appropriate response in order to reduce or limit the effect of an event after it happens or to prevent against the development of casualties, damage, and/or loss (Yazdani et al, 2012). The TOPSIS method helps decision-makers carry out analysis and comparisons in ranking their preference of the alternatives with vague or imprecise data (Yazdani et al., 2012). It is based on the concept that the chosen alternative should have the shortest distance from the positive-ideal solution and the longest distance from the negative-ideal solution (Secme et al., 2009; Gummus, 2009; Sun, 2010; Yue, 2011).

A study by Yang et al. (2009) uses a fuzzy evidential reasoning (ER) method to conduct maritime security assessments. Within this method, a subjective security-based assessment and management framework using fuzzy ER approaches was developed. The consequence parameter is a security parameter which can be derived from multiple risk parameters: will, damage capability, recovery difficulty, and damage probability. Here, *will* is the likelihood of a threat-based risk, which directly represents the lengths one goes through in taking a certain action. To estimate *will*, one may choose to use such linguistic terms such as "Very weak," "Weak," "Average," "Strong," and "Very strong." The combination of *damage capability* and *recovery difficulty* represents the consequence

severity of the threat-based risk. Specifically, *damage capability* indicates the destructive force/execution of a certain action, and *recovery difficulty* hints at the resilience of the system after the occurrence of a failure or disaster (Yang et al., 2009). The following linguistic terms can be considered as a reference to be used in subjectively describing the two sister parameters: "Negligible," "Moderate," "Critical," and "Catastrophic" for *damage capability* and "Easy," "Average," "Difficult," and "Extremely Difficult" for *recovery difficulty*. In this case, *damage probability* means the probability of the occurrence of consequences and can be defined as the probability that damage consequences happen given the occurrence of the event. One may choose to use such linguistic terms as "Unlikely," "Average," "Likely," and "Definite" to describe it (Yang et al., 2009; Yang et al., 2007).

2.7.2. Summary of Fuzzy Logic Methods

Xia et al, (2004) developed a methodology to address the dynamic nature of specific infrastructure aspects without including uncertainty. The method developed by McGill and Ayyub (2008) outlined a fuzzy approach to assess the effectiveness of security system capabilities from the terrorist perspective but did not look specifically at infrastructure characteristics or the natural threat perspective. Yazdani et al, (2012) added two new criteria, "detectability" and "reaction against event", into the traditional risk equation and input the new criteria into a fuzzy framework. Yang et al, (2009) further developed the variables used in the traditional risk equation to include new parameters based on terrorist attack for maritime transport and input these into a fuzzy evidential

reasoning framework. This method does not break down the variables into infrastructure specific subcategories.

2.8. Risk Considerations in Project Evaluation and Programming

Multi-criteria decision making uses any of several alternative methods including cost effectiveness, economic efficiency, the factor rating method, and the analytic hierarchy process. Economic efficiency can be calculated using the net present value, present worth of costs, or the benefit cost ratio. The factor rating method ranks different criteria based on subjective weighting. The analytic hierarchy process uses matrix multiplication of criteria weights to each alternative weight to derive the best option. The basic steps for conducting multi-criteria optimization are shown in Figure 2.6.

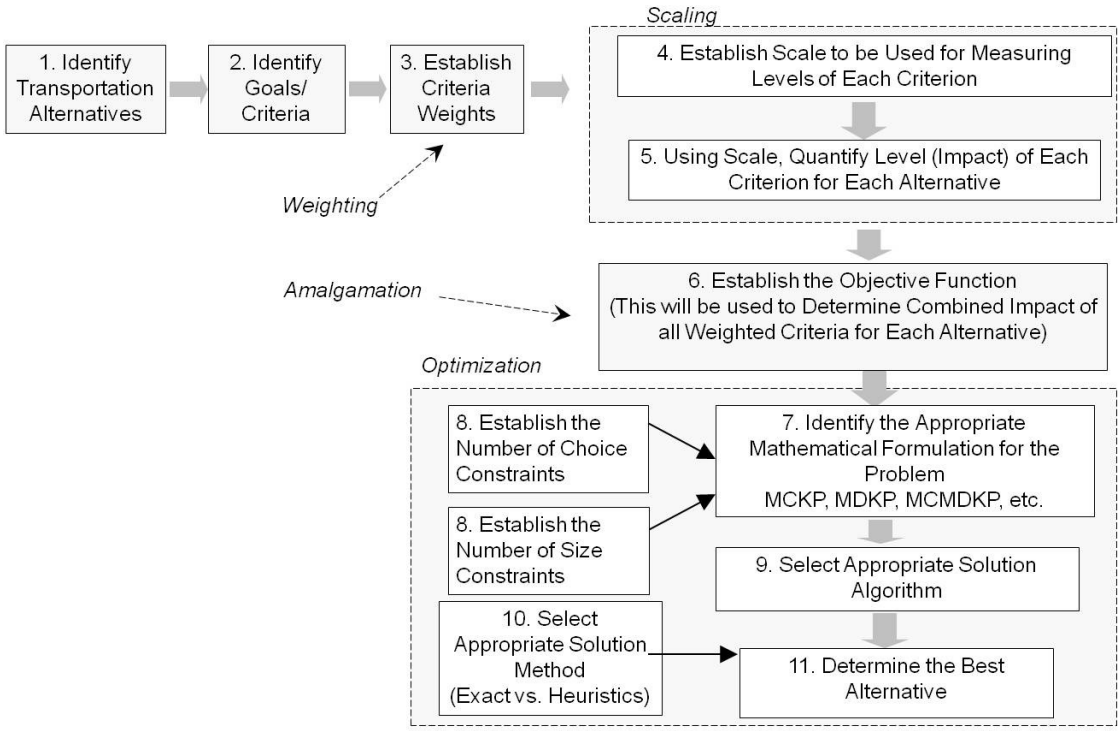


Figure 2.6. Steps for Conducting Multi-Criteria Optimization (Sinha and Labi, 2007).

Cellucci (2010) developed a method to prioritize proposed programs and projects for the U.S. Department of Homeland Security. The method uses a Program Prioritization Index (PPI), a simple metric to evaluate the value gained from pursuing certain proposed programs relative to others. It is a value-based model that captures the relative utility of one program over another by incorporating a utilitarian approach to provide the most "good" for the most people and property, while recognizing both political sensitivity and risk and cost-saving factors. The first factor incorporates the people protected from potential threat (typical occurrence). Points for this factor are assigned to the following number of people potentially protected: assign zero for zero people; one for 1-10 people; two for 11-100; three for 101-500 people; four for 501-1000 people; and five for 1001-100,000 people and an additional point for each 20,000 people potentially protected. The

second factor incorporates property protected from potential threat. The points for this factor are assigned to every $50M of property protected and the positive political impact generated (societal perception) as a result of a program/project's implementation. Zero points are assigned for "low"; five points for "medium"; and ten points for "high." The third factor incorporates the cost savings realized by DHS upon full implementation of the program where one point is assigned for each $1,000,000 saved (includes personnel plus resources). Finally, the last factor incorporates dollars requested/spent by DHS on the program/project where one point is assigned for each $1,000,000.

The PPI calculation is:

$$PPI = \frac{A+B+C+D}{E} \tag{21}$$

Where *A* is the people protected points; *B* is the property protected points; *C* is the societal perception points; *D* is the cost savings points; and *E* is the dollars requested/spent.

The higher the PPI value, the more value it potentially returns for a given DHS investment. For a risk-adjusted PPI, the PPI is multiplied by the "probability of success" of the program/project (e.g., obtain all stated objective(s)/specification(s)) expressed in a fraction ranging from 0% probability of success (0.0) to 100% probability (1.0). For example, 0.5 would relate to a 50% probability of success.

McGill et al. (2007) used the benefit-cost ratio technique to assess the cost effectiveness of proposed countermeasures and consequence mitigation strategies. In this case, the benefit of a risk mitigation action is the difference between the values of loss, conditional risk, or total annual risk before and after its implementation.

In planning for infrastructure security, many uncertainties arise pertaining to threat likelihood. Not planning for this uncertainty could lead to less-than-optimal decision-making. An inaccurate prediction of threat likelihood raises the risk of failure for infrastructure, therefore increasing the potential consequences. Uncertainty in accounting for security of infrastructure may also result in biased selections of alternative improvements and errant project prioritization. By making risk-informed decisions, stakeholders can more accurately compare levels of confidence against costs (Ford, 2011).

2.9. Gaps in the Literature

All methodologies employ varying definitions for key terms while incorporating differing factors in a myriad of combinations. Many factors, such as vulnerability and criticality, are so similar that they should not be considered separately. Additionally, many key factors, such as resilience, are missing from the risk assessment methodologies in the literature. Without strong definitions and key factors, making a case to fund security enhancements for transportation infrastructure based on current methods will be difficult.

As stated in a previous section, risk is a multidimensional concept which is often expressed as the Cartesian product in the context of risk analysis for critical infrastructure (McGill et al., 2008). The formula for risk expresses the interaction among the three factors of threat likelihood, vulnerability, and consequence, where dominant factors magnify risk and negligible factors diminish it (AASHTO, 2003). Different formulas,

such as models that add factors, fail to account for the factor interaction effects (Venna and Fricker, 2009).

2.10. Chapter Summary

This chapter provided a literature review of current risk assessment steps and methodologies. First, risk assessment was defined and the terms associated in quantifying risk were detailed. The different classifications of threat type were described and threat likelihood was characterized as the probability that an external or internal threat will occur. Resilience was outlined as a function of vulnerability and consequence as well. Various methods in the literature were analyzed for their robustness, and gaps were identified for future improvement. The next chapter illustrates the dissertation's framework for filling the gaps found in the literature review.

CHAPTER 3: METHODOLOGY

3.1. Introduction

As discussed in Section 2.8., traditional transportation infrastructure project evaluation uses a variety of performance measures that are related to the transportation asset, its operations, and its environment but does not consider directly possible reduction in the infrastructure damage and the resulting consequences in the event of a disaster. During the prioritization of investments, assets of low security do not receive the due attention they deserve. By incorporating the threat likelihoods, asset resilience, and disaster consequences, this chapter is based on the premise that the inclusion of these considerations in evaluation and prioritization introduces a much needed element of robustness in such tasks. However, the inclusion of security as a performance measure leads to an increase in the number of performance measures for the investment evaluation. Also, there is some uncertainty or variability associated with the threat occurrence, asset resilience, and disaster consequences. For these two reasons respectively, the framework presented in this chapter incorporates elements of multiple criteria decision making and fuzzy logic. This chapter presents a methodology to quantify the overall security level for an asset in terms of the threats it faces, its resilience to damage from such threats, and the consequences of the infrastructure damage if the threat occurs. The overall framework consists of the traditional steps in risk management and the specific contribution is in the part of the framework that measures the risk.

3.2. Proposed Definition of Security

For this dissertation, security can be defined as a function of threat likelihood, asset resilience and damage consequences. The security of a transportation asset is the lack of risk of damage from threats due to inherent structural or functional resilience.

3.3. Framework

The proposed security rating developed in this dissertation has three main inputs which are integral to risk assessment: threat likelihood, asset resilience, and disaster consequence. The output, security rating index, can be used to help in prioritizing assets for optimal security enhancement funding and for use in multi-criteria project evaluation (Figure 3.1).

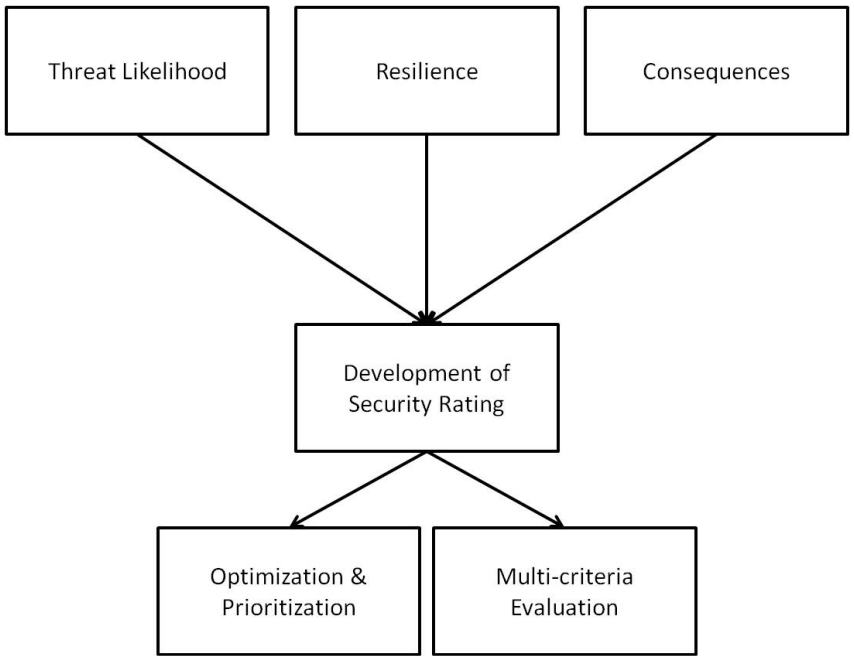


Figure 3.1. Proposed Methodology Framework

The definitions of the key inputs and terminology used in this dissertation are defined in Table 3.1.

Table 3.1. Terminology for Proposed Framework

Term	Definition
Asset	Specific transportation infrastructure
Resilience	The ability of the asset to withstand and recover from the threat
Threat Likelihood	The probability of a threat occurring that effects the asset
Consequence	The effects of the failure of an asset and its associated costs and damages
Factor	Plays an integral role in quantifying security of an asset
Measure	Quantifies how much the factor contributes to asset security
Attribute	Level of the measure rated on a scale to define the overall amount that the measure contributes to the factor

3.4. Security Factors

Each of the three main security factors (threat likelihood, asset resilience, and damage consequences) has measures that quantify how much each factor contributes to the overall security of an asset. Each measure is further decomposed into attributes that indicate the level of the measure rated on a scale to define the overall amount that the measure contributes to the security factor. Since the attributes of each measure have different units, the attribute data was scaled to account for these differences. Additionally, each measure is weighted for importance; therefore, a decision-maker can determine which measure plays a larger role in each specific security factor.

Each security factor is calculated as follows:

$$F_f = w_1 \cdot M_1 + \cdots + w_n \cdot M_n \quad (22)$$
$$f = 1....3$$
$$n = 1...n$$

Where F_f is a security factor; w_n is the weight/importance of measure n; and M_n is a measure of security factor F_f.

Each measure for a security factor follows the formulation below. Attributes that comprise a security measure are multiplied together and divided by the total number of attributes associated with a specific measure.

$$M_n = \frac{\prod_{i=1}^{s} s_i}{N_s} \quad (23)$$

Where M_n is a measure of security factor F_f; s_i is an attribute that contributes to the level of measure M_n, rated on a scale to define the overall amount that measure n contributes to the risk factor, F_f; and N_s is the number of attributes associated with measure n.

The detailed framework can be visualized in Figure 3.2. Each factor is shown with specific measures and each measure has associated attributes for the purpose of this dissertation.

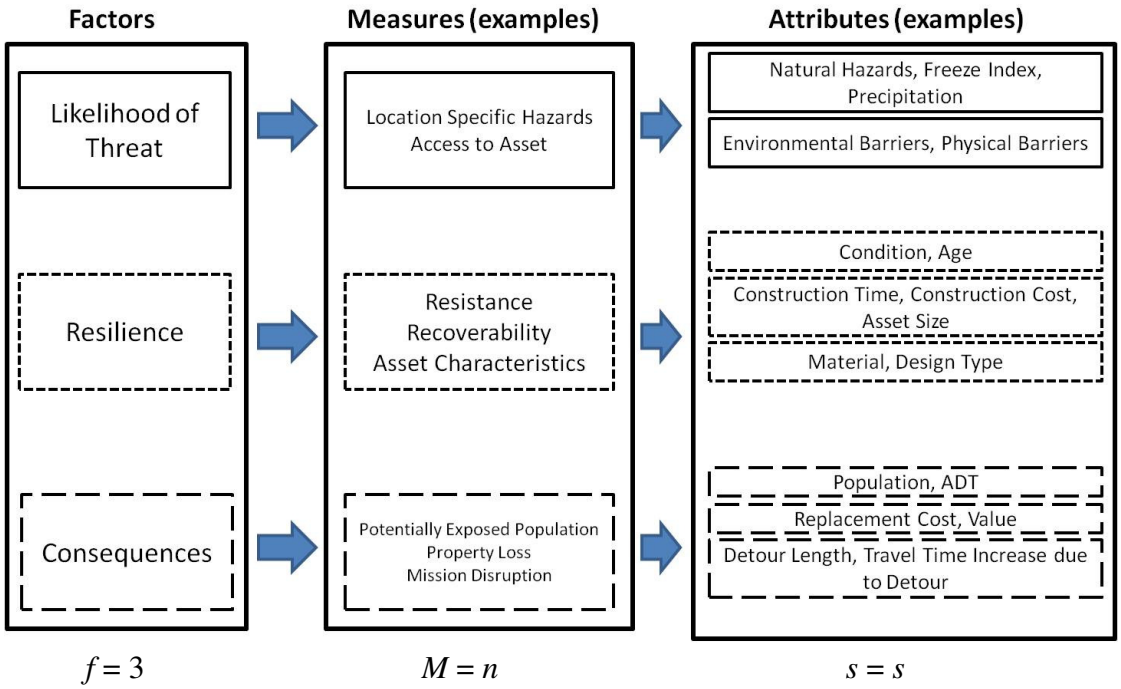


Figure 3.2. Detailed Framework

3.4.1. Methodology for Assessing Threat Likelihood

Threats to an asset can be categorized into three main groups: natural, man-made unintentional, and man-made intentional. Each of these groups contains many different threats to transportation assets as listed in Table 3.2.

Table 3.2. Examples of Threats to Transportation Infrastructure

	Natural	Man-made Unintentional	Man-made Intentional
Examples	Tornado Hurricane Earthquake Landslide Tsunami Volcano Flood Ice Lightning Sinkholes	Accidents Chemical Spills Collisions Overload	Arson Terrorism Vandalism
Data/models for occurrence prediction	Historical Data	Historical Data	Predictive models Literature

The measures associated with the threat likelihood factor in this study are the ease of access to the asset and location-specific hazards, such as earthquakes or floods. The following equation gives weights to each measure associated with the threat likelihood factor for an overall effect of threat likelihood on the security of an asset.

$$F_{1=TL} = w_1 \cdot M_1 + \cdots + w_n \cdot M_n \tag{24}$$

Where F_{TL} is the threat likelihood factor; w_1, w_n are the weight/importance for each threat likelihood measure; and M_1, M_n are measures of threat likelihood.

The measures are further broken down into attributes. The following equation relates the attributes that contribute to the factor measure.

$$M_n = \frac{\prod_{i=1}^{s} s_i}{N_s} \tag{25}$$

Where $M_n$is a measure for threat likelihood; s_i are the scaled attributes for measure n; and $N_{attribute}$ is the total number of attributes for measure n.

Each attribute is then scaled between one and five to account for different units of measure of each attribute for the purpose of the case study. These scales can be further refined by representative utility functions or value functions for each attribute. For example, the attributes could be scaled as shown Table 3.3., where a rating of five indicates a low level of contribution to the associated factor and one indicates a high level of contribution to the associated factor.

Table 3.3. Example Attribute Scale

Sample Attribute Levels	**Scale**
<50%	1
51%-74%	2
75%-84%	3
85%-94%	4
95%+	5

3.4.2. Resilience

Resilience is the ability of an asset to maintain essential functions with little or no disruption and to recover quickly when/if disrupted. The measures associated with the resilience factor in this study are how resistant the asset is to threats, the asset's ability to recover from a threat, and the asset characteristics. The following equation gives weights to each measure associated with the resilience factor for an overall effect of resilience on the security of an asset.

$$F_{2=R} = w_1 \cdot M_1 + \cdots + w_n \cdot M_n \quad (26)$$

Where F_R is the resilience factor; w_1, w_n are the weight/importance for each resilience measure; and M_1, M_n are measures of resilience.

The measures are further broken down into attributes. The resistance measure has two attributes, asset condition and asset age. Asset condition is defined as the physical asset condition of asset components. Asset age is defined as the age of the asset in year *t*. The following equation relates the attributes that contribute to the resistance measure.

$$M_n = \frac{\prod_{i=1}^{s} s_i}{N_s} \quad (27)$$

Where M_n is a measure for the resilience factor; s_i are the scaled attributes for measure *n*; and $N_{attribute}$ is the total number of attributes for measure *n*.

Each attribute is then scaled between one and five to account for different units of measure. In terms of resilience, a rating of five would indicate a high level of contribution to resilience and one would indicate a low level of contribution to resilience, opposite of the threat likelihood and consequence attribute scales.

3.4.3. Consequence

Consequence is the outcome of a threat towards a specific asset in terms of the damage to its surroundings. The following equation gives weights to each measure associated with the consequence factor for an overall effect of consequence on the security of an asset.

$$F_{3=C} = w_1 \cdot M_1 + \cdots + w_n \cdot M_n \quad (28)$$

Where F_C is the consequence factor; w_1, w_n are the weight/importance for each consequence measure; and M_1, M_n are measures of consequence.

The measures are further broken down into their attributes. The following equation relates the attributes that contribute to a measure of consequence.

$$M_n = \frac{\prod_{i=1}^{s} s_i}{N_s} \quad (29)$$

Where M_n is a measure for the consequence factor; s_i are the scaled attributes for measure n; and $N_{attribute}$ is the total number of attributes for measure n.

Each attribute is then scaled between one and five to account for different units of measure. A rating of five indicates a low level of contribution to the consequence factor and one indicates a high level of contribution to the consequence factor.

3.5. Security Rating

The security rating equation can take any one of several forms. Also, there are several ways by which the constituent factors could be weighted. For example, addition, subtraction, multiplication, a ratio, or some combination of the above: (i) $SR = F_{TL} + F_C - F_R$; (ii) $SR = F_{TL} \cdot F_C - F_R$; (iii) $SR = F_{TL} \cdot F_C \cdot F_R$; (iv) $SR = \frac{F_{TL} \cdot F_C}{F_R}$; (v) $SR = w_1(F_{TL} + F_C) - w_2 F_R$; (vi) $SR = {F_{TL}}^{\propto} \cdot {F_C}^{\beta} - {F_R}^{\lambda}$. Where SR is the security ratio; F_{TL} is the threat likelihood factor; F_C is the consequence factor; F_R is the resilience factor; and w_1, w_2, α, β, λ are factor weights. For purposes of this study, the security rating equation is shown below.

$$SR_a = \frac{F_{R_a}^{\alpha}}{\left(F_{TL_a}^{\delta} + F_{C_a}^{\lambda}\right)} \tag{30}$$

SR_a = security rating for asset a

F_{TLa} = threat likelihood factor of asset a

F_{Ca} = consequence factor of asset a

F_{Ra} = resilience factor of asset a

α = exponential weight of the resilience factor

δ = exponential weight of the threat likelihood factor

λ = exponential weight of the consequence factor

This form was chosen due to its ability to be understandably interpreted. The security factor of resilience, which has a positive connotation in terms of security, is divided by the security factors of consequence and threat likelihood, which have negative connotations in terms of security. An asset with high resilience would presumably be able to withstand a potential hazard therefore increasing its security level. An asset with large potential consequences and large threat likelihood would be associated with a lower security level. By formulating the equation in this arrangement, the larger the resilience and the smaller the consequences and threat likelihood, the greater the ratio. This would imply a high security rating. For example, if asset resilience increases due to improvements, threat likelihood is predicted to be low, and consequences decrease due to people moving away from the surrounding area, the security rating would increase. Therefore, the greater the security rating, the more secure the asset is. Each factor can be graphed against each other to identify assets of importance for security improvements to agencies or stakeholders as shown in the following three figures.

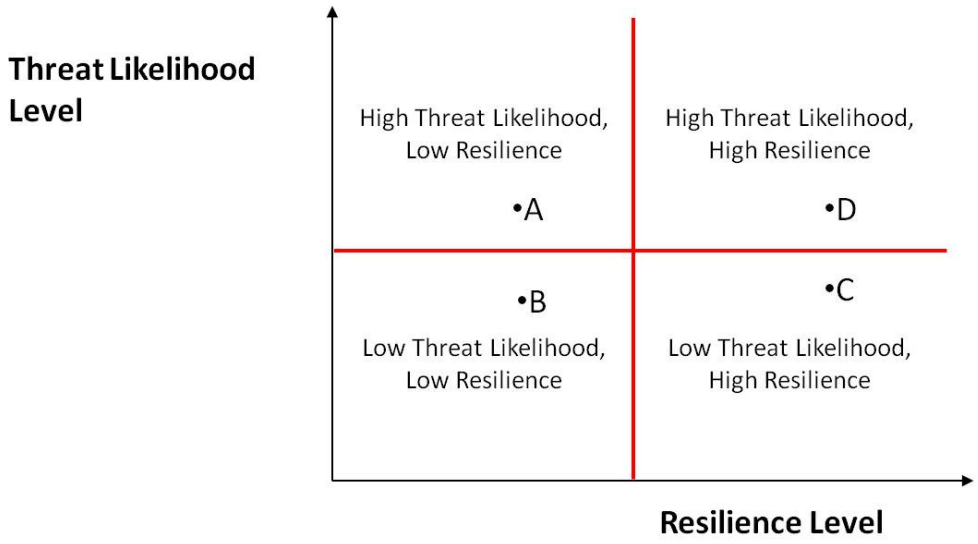


Figure 3.3. Threat Likelihood-Resilience Nomograph

In Figure 3.3., asset A has a high threat likelihood, indicating that a threat is imminent in the near future, and low resilience which would indicate the asset is not prepared for the oncoming threat. For example, if an asset was located in an area with a propensity for landslides and had not been brought up to code recently, the asset has a higher chance of failure. This asset would be of high importance to agencies and stakeholders when determining the prioritization for security improvements. Alternatively, Asset C has low threat likelihood and high resilience, making this asset prepared for any low probability threat that may occur. Agencies could give this asset lower priority for security improvements. Asset B and C could be given a medium priority for improvements since they have a mixture of good and bad qualities. Asset B has a low probability of threat occurring but is also not very resilient. In the case that a threat did occur, the asset would not be prepared to withstand it. Asset D has a high probability of threat and high resilience, therefore the asset is prepared for the threat, but it is located in a dangerous area.

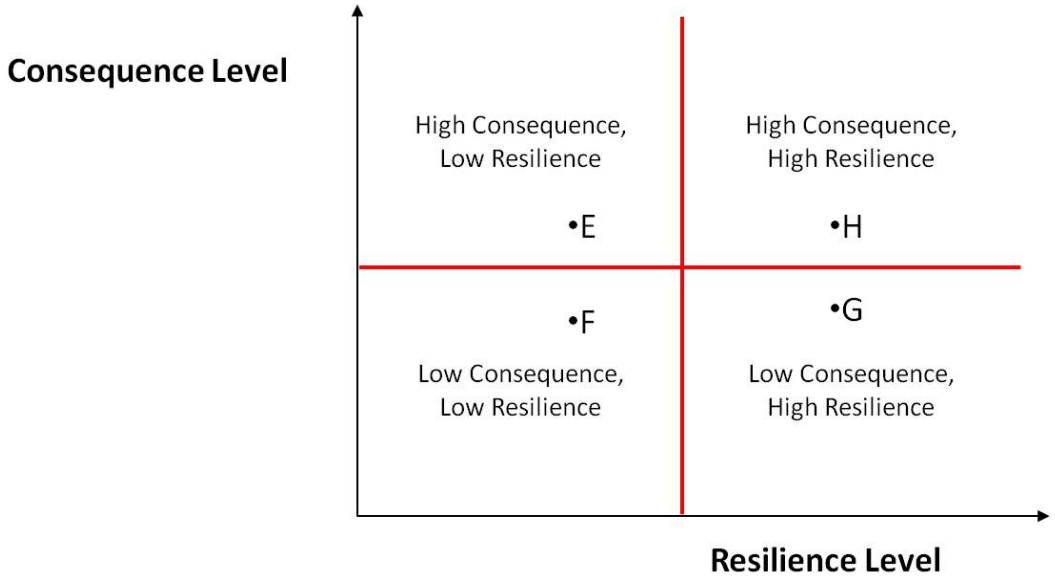


Figure 3.4. Consequence-Resilience Nomograph

In Figure 3.4., asset G has a low consequence level and high resilience indicating that if a threat did occur, the asset would be able to withstand it and there would be minimal consequences. This asset would be given less priority than asset E. Asset E has a high consequence level and low resilience level. Therefore, if a threat occurred, the asset would not be able to withstand it; and its failure would lead to high consequences. For example, a bridge that has not been maintained properly, is designed poorly, and is located near residences with a high volume of traffic could cause great damage if it failed. Agencies or stakeholders would need to focus on improving this asset in order to make it more resilient to the threat and therefore reduce the potential consequences. Assets F and H have a mixture of good and bad factors that play a role in their security. Asset F has a low resilience level and low consequence level indicating that the asset could potentially fail if a threat occurred but would not cause much damage in terms of consequences. Asset H has a high level of consequences but counters it with a high level

of resilience. This asset has the ability to withstand a threat and would therefore prevent consequences.

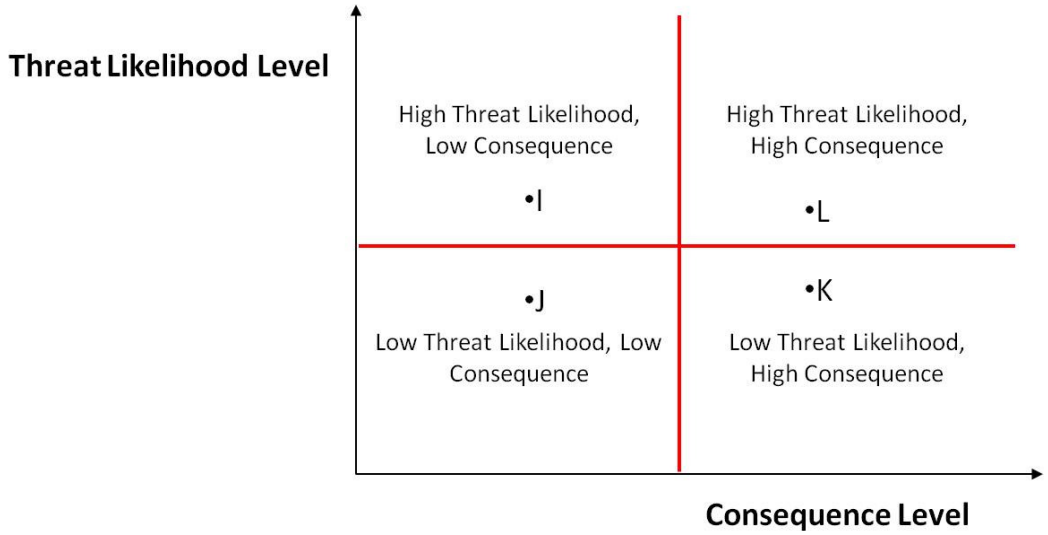


Figure 3.5. Threat Likelihood-Consequence Nomograph

In Figure 3.5., asset L has a high probability of threat occurring and high consequences should the asset fail. This asset should be given priority for security improvements to make sure it is very resilient in order to withstand the impending threats and lowering resulting consequences. Asset J has a low probability of threat occurring and low consequences, meaning it can be given a lower priority than other assets such as I and K which have more cause for improvements. Asset I has a high probability of threat occurrence but a low consequence level. This indicates that should a threat happen and the asset fails, the consequences would be minimal. For example, this asset may be located in a desert where no one resides. This means that consequences would not be high. Finally, asset K has a low probability of threat occurring but a high consequence level. If this asset failed, consequences would be devastating; but since threats are

minimal, it would have a low probability of failing and therefore could be placed in a medium priority level.

Additionally, a three-dimensional representation can be derived from these three factors to better show their interactions (Figure 3.6.). An asset with high threat likelihood, high consequences, and low resilience (the black square) would require agencies to focus on this asset in order to make sure it is more resilient, reducing the consequences of impending threats. Assets with high resilience, low consequences, and low threat likelihood (the off-white square) are of lesser priority for security improvements than those with low threat likelihood, low consequence, and low resilience (the gray square).

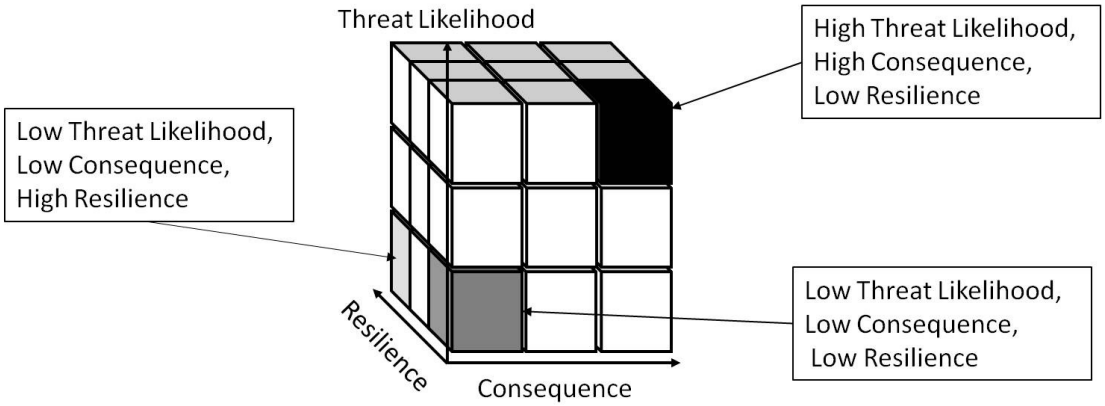


Figure 3.6. Three Dimension Representation of Security Rating Factors

The security rating can be placed on a scale and interpretations made as seen in the below figure and table below.

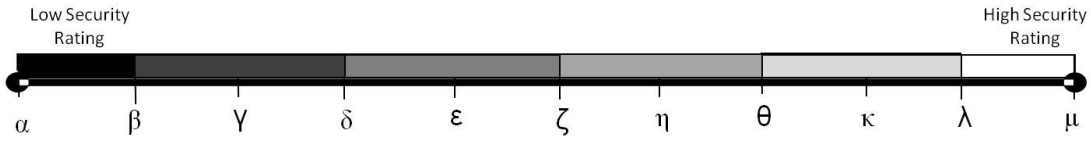


Figure 3.7. Security Rating Scale

Table 3.4. Interpretation of Security Rating

Security Rating	Interpretation
≤β	Indicates very high security improvement needs and low resilience thus immediate action should be undertaken to enhance resilience and thus reduce the possible consequences.
β-δ	Indicates high security improvement needs of the asset. The agency should be ready to undertake actions to enhance resilience and thus to reduce the possible consequences of the asset failing.
δ-ζ	Indicates medium-to-high security improvement needs. Facilities within this range can be monitored at a frequency slightly exceeding standard frequency. The risk of failure can be tolerated until a normal capital project (to enhance resilience and thus reduce consequences, among other benefits) is carried out.
ζ-θ	Indicates low-to-medium security improvement needs. Unexpected failure can be avoided during the remaining service life of the asset by performing standard scheduled inspections with due attention to specific design features that influence the assets possible consequences.
θ-λ	Indicates low security improvement need. Often reflective of the likelihood of threat to a civil engineering system built to the current design standards in a low threat likelihood environment.
λ-μ	Indicates little or no security improvement needs.

3.5.1. Expert Opinion

Expert opinion can be defined as the formal judgment of experts on a matter in which their advice is sought; an opinion could mean a judgment of a belief that is based on uncertain information or knowledge (Ayyub, 2001). Opinions are subjective assessments, evaluations, impressions, or estimations of the quality or quantity of something of interest that seems true, valid, or probable in the expert's view. The first structured methods for expert opinion elicitation were done by the Research and Development Corporation (RAND) (Ayyub, 2001). Elicitation methods include: the indirect elicitation, direct method, and parametric estimation. Multiple methods are available to synthesize expert opinion: the Delphi Method, scenario analysis, scientific

heuristics, and rational consensus being among them. In some cases, expert opinion in the form of subjective probabilities of an event need to be combined into a single value or intervals for their use in probabilistic and risk analyses (Ayyub, 2001). To successfully combine the opinions of different experts there are two main methodologies: mathematical and consensus. Mathematical methods, specifically, are based on assigning equal or different weights to expert opinion (Clemen, 1989; Ferrell, 1985), while consensus methods rely on mutual agreement.

Expert opinion can be used to build frequency or probability distributions when data is unavailable (Ford, 2011). In order to accomplish this goal, the following methodologies can be used: the Extended Pearson Turkey Method, Four Point Bracket Method, reference lotteries, and/or paired comparisons of situations (Clemen and Reilly, 2001). When working with expert opinion, caution should be taken to remove expert opinion biases in the estimations. Within this framework, experts were consulted to help determine measures for specific factors, scales for security attributes, and fuzzy logic membership function ranges.

3.6. Chapter Summary

This chapter presented a methodology to quantify the overall security level for an asset in terms of threat likelihood, asset resilience, and the consequences in the event of system damage due to threat occurrence. This methodology addresses the risk measurement aspect of the traditional risk management framework. The next chapter uses this methodology in an asset-level case study.

CHAPTER 4: ASSET LEVEL CASE STUDY

4.1. Introduction

Asset-level analysis is important to maintain and increase the security of transportation networks. Infrastructure should be analyzed at the asset-level due to the differences between asset types, location specific characteristics, and physical characteristics. Each asset provides a different combination of measures and attributes which should be closely analyzed to gain information on an asset's security. For example, an asset that is located in an area with propensity to earthquakes and near a large population would have a different security rating than an asset in an area with low earthquake occurrence and a location in the middle of a desert. Due to the range of combinations for each asset, an asset-level analysis must be completed to identify assets in need of security improvements.

Bridge #8868, the JFK Bridge in Jeffersonville, Indiana, was chosen as a sample case study to demonstrate how the security rating function works with associated measures, attributes, and attribute scales (Figure 4.1).

Figure 4.1. JFK Bridge, Structure No. 8868, Clark County, Jeffersonville, IN

4.2. Data and Assumptions

Data was taken from the National Bridge Inventory (NBI) database for the state of Indiana for Bridge No. 8868. Assumptions were made to carry out the case study. The construction time was based on the bridge size. Earthquakes were identified as the threat for the example and the probability of earthquake threat was equal to the amount of historical earthquake epicenters found in the county the asset resides in. Environmental barriers were assumed to be waterways under a bridge and physical barriers were assumed to be roadways under the bridge. The detour travel speed was assumed to be 45mph and all weights in the security rating equation (α, δ, λ) were assumed to be equal.

4.3. Factor Analysis

4.3.1. Threat Likelihood Factor Computation for the JFK Bridge Case Study

The measures associated with the threat likelihood factor in this case study are the ease of access to the asset and location-specific hazards, which include earthquakes or floods. The access-to-asset measure plays a role in an asset's security and is pertinent

when considering terrorist attacks. Some infrastructure hold iconic status to a country or group. This symbolic infrastructure could therefore be targeted by terrorists for the devastating impact of losing such a meaningful structure. The location-specific data, which focuses on location of an asset and what hazards are typical in that area, will be different depending on where each asset is situated. The following equation gives weights to each measure associated with the threat likelihood factor for an overall effect of threat likelihood on the security of an asset.

$$F_{TL} = w_{access-to-asset} \cdot M_{access-to-asset} + w_{location} \cdot M_{location} \quad (31)$$

Where F_{TL} is the threat likelihood; $w_{access\text{-}to\text{-}asset}$ is the weight/importance for access measure; $M_{access\text{-}to\text{-}asset}$ is the access to asset measure; $w_{location}$ is the weight/importance of the asset location; $M_{location}$ is the location specific hazards measure.

The measures are further broken down into attributes. The access-to-asset measure has two attributes: environmental barriers and physical barriers. Environmental barriers are natural barriers that keep the public and vehicles away from an asset; physical barriers are man-made barriers that keep the public and vehicles away from an asset. The following equation relates the attributes that contribute to the access-to-asset measure.

$$M_{access-to-asset} = \frac{s_{environmental} \cdot s_{physical}}{N_{attributes}} \quad (32)$$

Where $M_{access\text{-}to\text{-}asset}$ is the access-to-asset measure; $s_{environmental}$ is the environmental barrier scaled attribute; $s_{physical}$ is the physical barrier scaled attribute; and $N_{attribute}$ is the number of attributes for the access to asset measure.

The access-to-asset attributes are scaled as shown in Table 4.1.

Table 4.1. Attribute Scales for Access-to-Asset

Environmental Barriers	**Scale**
None	5
One	3
2+	1

Physical Barriers	**Scale**
None	5
One	3
2+	1

The location-specific hazards measure could have the following attributes: natural hazards, freeze index, and precipitation. Natural hazards are defined as location-specific hazards such as earthquakes or hurricanes. The freeze index is the cumulative number of degree-days when air temperatures are below and above zero degrees Celsius in the area around the asset. Precipitation is measured in 100th inches of rainfall at the asset location. The following equation relates the attributes that contribute to the location-specific hazards measure.

$$M_{location} = \frac{s_{natural} \cdot s_{freeze} \cdot s_{precipitation}}{N_{attributes}} \quad (33)$$

Where $M_{location}$ is the location-specific hazards measure; $s_{natural}$ is the natural hazard scaled attribute; s_{freeze} is the county freeze index scaled attribute; $s_{precipitation}$ is the county precipitation scaled attribute; and $N_{attribute}$ is the number of attributes for the location specific hazards measure.

The location specific hazard attributes are scaled as shown in Table 4.2 based on expert opinion.

Table 4.2. Attribute Scales for Location-Specific Hazard

Natural Hazard Probability (% chance of hazard)	**Scale**	**Freeze Index**	**Scale**	**Precipitation (100^{th} inches)**	**Scale**
<50%	1	<115	1	<37	1
51%-74%	2	115-263	2	37-39	2
75%-84%	3	263-462	3	39-42.4	3
85%-94%	4	462-661	4	42.4-45	4
95%+	5	661+	5	45+	5

Threat likelihood data for the JFK Bridge are shown in Table 4.3. The threat likelihood factor equates to 2.67 using the equations (34-36) for the measures shown below.

Table 4.3. JFK Bridge Threat Likelihood Factor Data

Measure	Attributes	Data	Scaled Attributes	Measure Results
Access to Asset	Env Barriers	Over river	3	4.5
	Physical Barriers	Roadway underneath	3	
Location Specific Hazards	Natural Hazards	Earthquake epicenter	1	1.67
	County Freeze Index	30	1	
	County Precipitation	45.84	5	

$$M_{access-to-asset} = \frac{s_{environmental} \cdot s_{physical}}{N_{attributes}} = \frac{3 \cdot 3}{2} = 4.5 \quad (34)$$

$$M_{location} = \frac{s_{natural} \cdot s_{freeze} \cdot s_{precipitation}}{N_{attributes}} = \frac{1 \cdot 1 \cdot 5}{3} = 1.67 \quad (35)$$

$$F_{TL} = w_{access-to-asset} \cdot M_{access-to-asset} + w_{location} \cdot M_{location} = 0.5 \cdot 4.5 + 0.5 \cdot 1.67 = 2.67 \quad (36)$$

4.3.2. Resilience Factor Computation for the JFK Bridge Case Study

The measures associated with the resilience of an asset are: the asset resistance to hazards, asset recoverability after damage, and the asset's physical characteristics. An asset's ability to resist and recover from a hazard gives an indication as to how long repairs will take, and therefore, how much it will cost to fix. Asset physical characteristics will also play a role in predicting how well an asset can withstand a hazard. For example, an older asset may not be up to current building codes and therefore not structurally advanced to withstand an earthquake or flood. The following equation gives weights to each measure associated with the resilience factor for an overall effect of resilience on the security of an asset.

$$F_R = w_{resistance} \cdot M_{resistance} + w_{recoverability} \cdot M_{recoverability} + w_{characteristics} \cdot M_{characteristics} \quad (37)$$

Where F_R is the resilience factor; $w_{resistance}$ is the weight/importance of asset resistance; $M_{resistance}$ is the measure of asset resistance; $w_{recoverability}$ is the importance/weight of asset recoverability; and $M_{recoverability}$ is the measure of asset recoverability; $w_{characteristics}$ is the weight/importance of asset characteristics; and $M_{characteristics}$ is the asset characteristic measure.

The measures are further broken down into attributes. The resistance measure has two attributes: asset condition and asset age. Asset condition is defined as the physical asset condition of asset components. Asset age is defined as the age of the asset in year *t*. The following equation relates the attributes that contribute to the resistance measure.

$$M_{resistance} = \frac{s_{condition_i} \cdot s_{age_t}}{N_{attributes}} \quad i = 1 \ldots I \tag{38}$$

Where $M_{resistance}$ is the measure of asset resistance; $s_{conditioni}$ is the condition scaled attribute for i asset components; s_{aget} is the scaled attribute for asset age in year t; and $N_{attribute}$ is the number of attributes for the resistance measure.

The resistance attributes are scaled as shown in Table 4.4. In this case, the scaled rating of five implies a greater contribution to resilience as opposed to the attributes associated with the threat likelihood and consequence factors.

Table 4.4. Scaled Attributes for the Resistance Measure

Condition (0-9)	**Scale**
7-9	5
6	4
5	3
3-4	2
1-3	1

Age (years)	**Scale**
<5	5
5-10	4
10-19	3
19-70	2
70+	1

The bridge rating scale used in the NBI database is shown in Table 4.5. A histogram of bridge ages in Indiana is shown in Figure 4.2. These data and expert opinion were used to determine the attribute scales.

Table 4.5. National Bridge Inventory Rating Scale

Rating	Description
9	Excellent Condition
8	Very Good Condition-no problems noted
7	Good Condition-some minor problems
6	Satisfactory Condition-structural elements show minor deterioration
5	Fair Condition-all primary structural elements are sound but may have minor corrosion, cracking or chipping. May include minor erosion on bridge piers.
4	Poor Condition - advanced corrosion, deterioration, cracking or chipping. Also significant erosion of concrete bridge piers.
3	Serious Condition - corrosion, deterioration, cracking and chipping, or erosion of concrete bridge piers have seriously affected deck, superstructure, or substructure. Local failures are possible.
2	Critical Condition - advanced deterioration of deck, superstructure, or substructure. May have cracks in steel or concrete, or erosion may have removed substructure support. It may be necessary to close the bridge until corrective action is taken.
1	"Imminent" Failure Condition - major deterioration or corrosion in deck, superstructure, or substructure, or obvious vertical or horizontal movement affecting structure stability. Bridge is closed to traffic but corrective action may put back in light service.
0	Failed Condition - out of service - beyond corrective action
N	Not applicable

Source: Federal Highway Administration, National Bridge Inventory

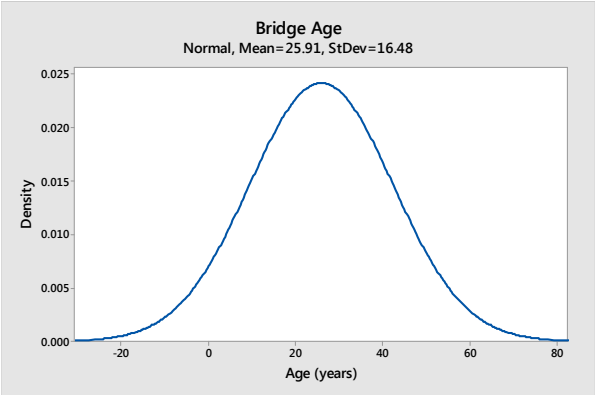


Figure 4.2. Probability Distribution of Indiana Bridge Age

The recoverability measure has three attributes: construction time, construction cost, and asset size. Asset time is defined as the amount of time needed to reconstruct the asset in case of total failure. Construction cost is the amount of dollars needed to construct the asset. Asset size is the area the asset takes up (ft^2, lane-miles). These attributes play a role in how quickly an asset can recover from hazard damage. For

example, the greater the size of an asset, the more it will cost for materials and repairs and the longer it may take to fix. The following equation relates the attributes that contribute to the recoverability measure.

$$M_{recoverability} = \frac{s_{time} \cdot s_{size} \cdot s_{cost}}{N_{attributes}} \quad (39)$$

Where $M_{recoverability}$ is the measure of asset recoverability; s_{time} is the time is takes to reconstruct the asset; s_{size} is the size of the asset; s_{cost} is the construction cost of the asset; and $N_{attribute}$ is the number of attributes for the recoverability measure.

The recoverability attributes are scaled as shown in Table 4.6. Histograms of construction cost and size for Indiana bridges are seen in Figures 4.3. and 4.5. This data and expert opinion determined the recoverability attribute scales for this case study.

Table 4.6. Recoverability Measure Scaled Attributes

Construction Time (yrs)	**Scale**
<0.3	5
0.4-0.9	4
1-2	3
2.1-5	2
5.1+	1

Construction Cost	**Scale**
<$1.98M	5
$1.98M-$4.57M	4
$4.57M-$9.83M	3
$9.83M-$21.8M	2
$21.8M+	1

Asset Size (ft^2)	**Scale**
<11,440	5
11,440-31,747	4
31,748-78,373	3
78,373-235,914	2
235,914+	1

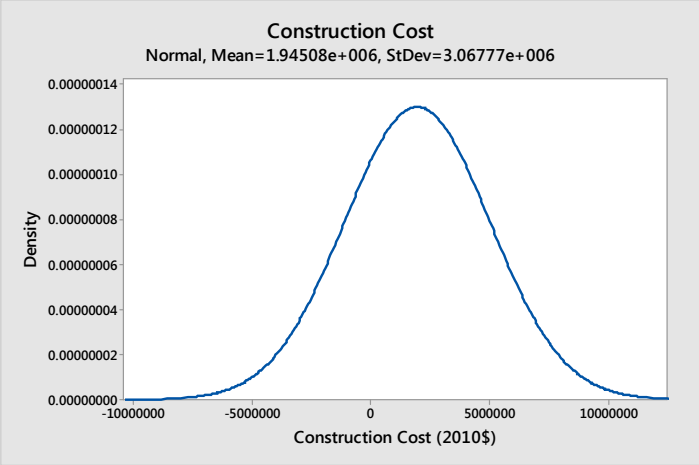


Figure 4.3. Probability Distribution of Indiana Bridge Network Construction Cost

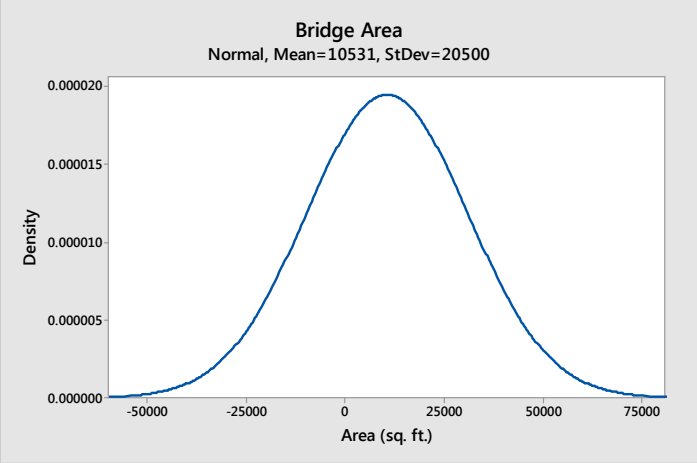


Figure 4.4. Probability Distribution of Indiana Bridge Network Size

The asset characteristic measure has two attributes: asset material and asset design type. Asset material is the dominant type of material the asset is constructed from. Asset design type is the design type of the asset. The following equation relates to the attributes that contribute to the asset characteristic measure.

$$M_{characteristics} = \frac{s_{material} \cdot s_{design}}{N_{attributes}} \quad (40)$$

Where $M_{characteristics}$ is the measure for asset characteristics; $s_{material}$ is the scaled attribute for asset material; s_{design} is the scaled asset design type; and $N_{attributes}$ is the number of attributes for the asset characteristic measure.

The asset attribute scales for the characteristics measure are shown below. Asset characteristics are important for determining if an asset is resilient based on its physical characteristics. For example, a concrete or steel bridge may be able to withstand more fire damage than a timber bridge. Concrete, steel, and timber represent over 98% of the materials used for bridge construction in the United States (Smith et al, 1997). In a study by Smith et al. (1997), bridge materials were rated using expert opinion and the analytical hierarchy process. State department of transportation engineers, private consulting engineers, and local highway officials from Mississippi, Virginia, Washington, and Wisconsin were interviewed for their expert opinion. In each state, a group of four to twelve individuals were interviewed. The results showed that based on the factors of: performance measures of material lifespan, past performance, maintenance requirements, resistance to natural deterioration, initial cost, and lifecycle cost, that prestressed concrete was the material of choice followed by reinforced concrete, steel, and timber (Smith et al, 1997). This study was used to determine the scale for the bridge material attribute (Table 4.7.). Bridge types also possess positive and negative aspects of their design. It is very important to select the most appropriate bridge type for a site to account for cost-effectiveness and area characteristics (USDOT, 2012). Table 4.8. below lists some examples of strengths and weaknesses for many bridge types.

Table 4.7. Asset Characteristic Measure Scaled Attributes

Material	**Scale**
Prestressed Concrete	5
Reinforced Concrete	4
Steel	3
Other	2
Wood	1

Design Type	**Scale**
Slab	5
Box Beam	4
Stringer, Girder	3
Truss	2
Cable-stayed, Arch, Suspension	1

Table 4.8. Bridge Design Type Strengths and Limitations

Bridge Type	Strengths	Limitations
Beams	• Unit cost of rolled beams low due to simple fabrication • Details less expensive • Economical in short span ranges	• Higher unit weights due to rolled beams
Girders	• Multi-girder composite construction accounts for deck strength • Deck girders offer flexibility of roadway width	• Welding led to cracks • Fracture critical • Through girder system limited to superstructure depth restriction
Trusses	• Used when unrestricted vertical clearance below bridge • Economical substructures • Easy to widen	• Fracture critical • Widening limited to structural capacity • Not cost-effective for span under 450 feet • Labor intensive
Cable-stayed	• Edge girders carry bending between stay cable anchorages plus axial • Compressive forces additive from end longest cables toward towers	• Edge girder design not controlled by bending but by compressive forces imparted by stay cables, requiring heavier section to avoid buckling
Suspension	• Rely on high-strength cables as major structural elements • Towers significantly shorter than those required for cable-stayed	• Not economical until main span length exceeds 3,000 feet • Require large expensive steel castings • Specialized erection process
Arch	• Economical for very long spans • Used to cross deep valley with steep walls • High performance steel used to reduce fractures • Redundancy reduces fracture critical status	• Foundation costs increase for deep foundations • Tied arches are fracture critical • Not economical after 900 feet length • Fracture critical • Complex to erect

Source: USDOT (2012)

The resilience measures, attributes, and scales for the JFK Bridge can be seen in Table 4.9. Equations (41-44) used the data to compute each measure value and input for the resilience factor equation. The resilience factor equates to 9.13.

Table 4.9. JFK Bridge Resilience Factor Data

Measure	Attributes	Data	Scaled	Results
Resistance	Condition	Deck: 6	4	24
		Superstructure: 5	3	
		Substructure: 6	4	
	Age	83 yrs	2	
Recoverability	Const. Time	2yrs	2	0.66
	Const. Cost	$45.2M	1	
	Asset Size	267,466 ft^2	1	
Asset Characteristics	Material	Continuous steel	3	3
	Design Type	Truss Bridge	2	

$$M_{resistance} = \frac{s_{condition_i} \cdot s_{age_t}}{N_{attributes}} = \frac{4 \cdot 3 \cdot 4 \cdot 2}{4} = 24 \quad (41)$$

$$M_{recoverability} = \frac{s_{time} \cdot s_{size} \cdot s_{cost}}{N_{attributes}} = \frac{2 \cdot 1 \cdot 1}{3} = 0.66 \quad (42)$$

$$M_{characteristics} = \frac{s_{material} \cdot s_{design}}{N_{attributes}} = \frac{3 \cdot 2}{2} = 3 \quad (43)$$

$$F_R = w_{resistance} \cdot M_{resistance} + w_{recoverability} \cdot M_{recoverability} + w_{characteristics} \cdot M_{characteristics} = 0.33 \cdot 24 + 0.33 \cdot 0.66 + 0.33 \cdot 3 = 9.13 \quad (44)$$

4.3.3. Consequence Factor Computation for the JFK Bridge Case Study

The measures associated with the consequences of bridge failure due to a hazard are: the potentially exposed population around the asset, the property lost due to the bridge failure, and the effects of mission disruption due to a closed bridge. For example,

people that live near the bridge may rely on the bridge to allow them to travel across a river, and if the bridge is closed, they may need to travel out of their way to cross the river on another bridge. Consequences could also arise from the bridge collapsing while people are traveling over it and could ruin anything under or near the bridge from falling debris. Additionally, the loss of a bridge will detract from an agency's total infrastructure value and lead to repair costs. The following equation gives weights to each measure associated with the consequence factor for an overall effect of consequence on the security of an asset.

$$F_C = w_{population} \cdot M_{population} + w_{property} \cdot M_{property} + w_{disruption} \cdot M_{disruption} \quad (45)$$

Where F_C is the consequence factor; $w_{population}$ is the potentially exposed population importance; $M_{population}$ is the potentially exposed population measure; $w_{property}$ is the property loss importance; $M_{property}$ is the property loss measure; $w_{disruption}$ is the mission disruption importance; and $M_{disruption}$ is the measure of mission disruption.

The measures are further broken down into their attributes. The potentially exposed population measure has two attributes: population around the asset and average daily traffic (ADT). The population around the asset is defined as the number of people in the area surrounding an asset. The following equation relates to the attributes that contribute to the potentially exposed population measure.

$$M_{population} = \frac{s_{population} \cdot s_{ADT}}{N_{attributes}} \quad (46)$$

Where $M_{population}$ is the potentially exposed population measure; $s_{population}$ is the scaled population around the asset attribute; s_{ADT} is the average daily traffic on the asset; and $N_{attributes}$ the number of attributes for the potentially exposed population measure.

The potentially exposed population attributes are scaled as shown in Table 4.10. The county population where the asset is located was used as the potentially exposed population for the case study.

Table 4.10. Potentially Exposed Population Measure Scaled Attributes

ADT	**Scale**
<6,920	1
6,921-17,950	2
17,951-36,710	3
36,711-79,520	4
79,921+	5

County Population	**Scale**
<38,075	1
38,076-84,964	2
84,965-182,791	3
182,792-484,564	4
484,565+	5

The property loss measure has two attributes: replacement cost and value. The replacement cost is the total cost to replace the asset. Value is the worth of the asset to stakeholders. The following equation relates the attributes that contribute to the property loss measure.

$$M_{property} = \frac{s_{rcost} \cdot s_{value}}{N_{attributes}} \quad (47)$$

Where $M_{property}$ is the property loss measure; s_{rcost} is the scaled replacement cost attribute; s_{value} is the scaled asset value attribute; and $N_{attributes}$ is the number of attributes for the property loss measure.

The scaled property loss attributes are shown in Table 4.11. Both replacement cost and value attributes were grouped based expert opinion and INDOT data distributions.

Table 4.11. Property Loss Measure Scaled Attributes

Replacement Cost	**Scale**
<$11,000	1
$10,001-$1.49M	2
$1.5M	3
$1.5M-$119M	4
$120M+	5

Value (EDMC)	**Scale**
<$2.06M	1
$2.06M-5.5M	2
$5.51M-$12.8M	3
$12.81M-$38M	4
$38M+	5

The mission disruption measure also has two attributes: detour length and travel time increase due to detour. The detour length is measured by the miles driven to travel around the asset to continue to a destination. Travel time increase due to the detour is the increase in travel time due to traveling around the failed asset. Time has no intrinsic value, but in terms of time saved due to arriving at a destination early, value is given to the ability to perform other tasks during this additional time (Sinha and Labi, 2007). In this case, saved travel time would provide a benefit to drivers while increased travel times would cost them time and energy. Therefore, mission disruption identifies increase in travel time due to a detour a consequence of impassable infrastructure. The following equation relates to the attributes that contribute to the mission disruption measure.

$$M_{disruption} = \frac{s_{detour} \cdot s_{tt}}{N_{attributes}} \tag{48}$$

Where $M_{disruption}$ is the mission disruption measure; s_{detour} is the scaled detour length attribute; s_{tt} is the scaled travel time increase due to the detour attribute; and $N_{attribute}$ is the number of attributes for the mission disruption measure.

The mission disruption attributes are scaled in Table 4.12.

Table 4.12. Mission Disruption Measure Scaled Attributes

Detour Length (miles)	**Scale**
<2	1
3	2
6	3
8	4
10+	5

Travel Time Inc. (min)	**Scale**
<3	1
3-5	2
5-8	3
8-10	4
10+	5

The data for the JFK Bridge consequence factor can be seen in Table 4.13. The consequence factor equates to 4.29 using equations (49-52).

Table 4.13. JFK Bridge Consequence Factor Data

Measure	Attributes	Data	Scaled	Results
Potentially Exposed Population	Population	Jeffersonville: 27,362 Clark County: 96,472	3	3
	AADT	15,200	2	
Property Loss	Replacement Cost	$36.1M	4	8
	EDMC Value	$18.63M	4	
Mission Disruption	Detour Length (miles)	3.11	2	2
	Inc in travel time due to detour	4.15 min	2	

$$M_{population} = \frac{s_{population} \cdot s_{AADT}}{N_{attributes}} = \frac{3 \cdot 2}{2} = 3 \quad (49)$$

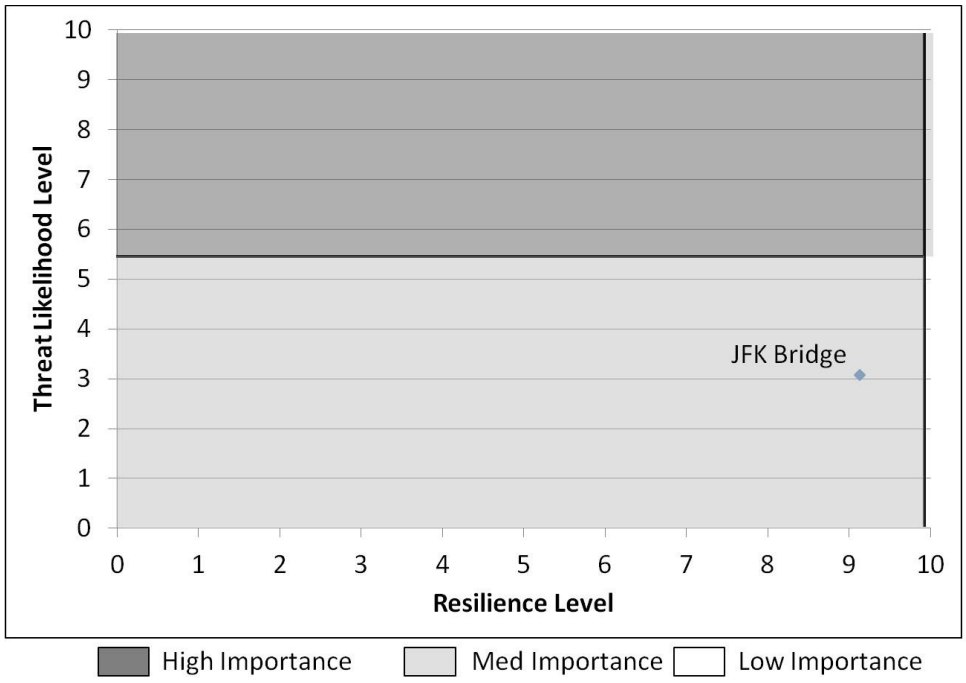
$$M_{property} = \frac{s_{rcost} \cdot s_{value}}{N_{attributes}} = \frac{4 \cdot 4}{2} = 8 \quad (50)$$

$$M_{disruption} = \frac{s_{detour} \cdot s_{tt}}{N_{attributes}} = \frac{2 \cdot 2}{2} = 2 \quad (51)$$

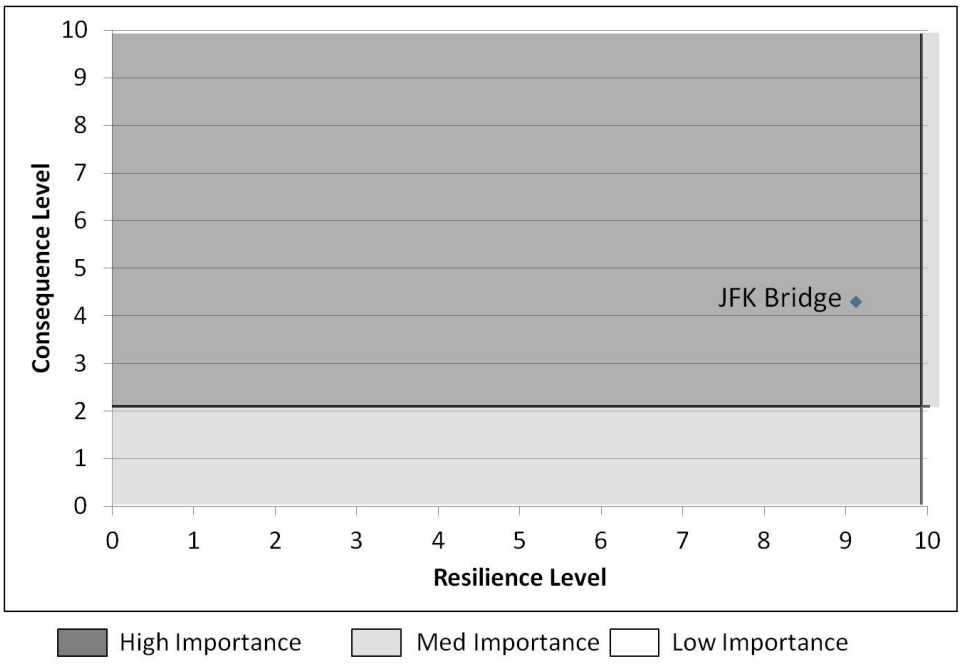
$$F_C = w_{population} \cdot M_{population} + w_{property} \cdot M_{property} + w_{disruption} \cdot M_{disruption}$$
$$= 0.33 \cdot 3 + 0.33 \cdot 8 + 0.33 \cdot 2 = 4.29 \quad (52)$$

The individual security factors for the JFK Bridge are graphed for further analysis and lie in the medium (gray) to high (dark gray) importance ranges as delineated by the

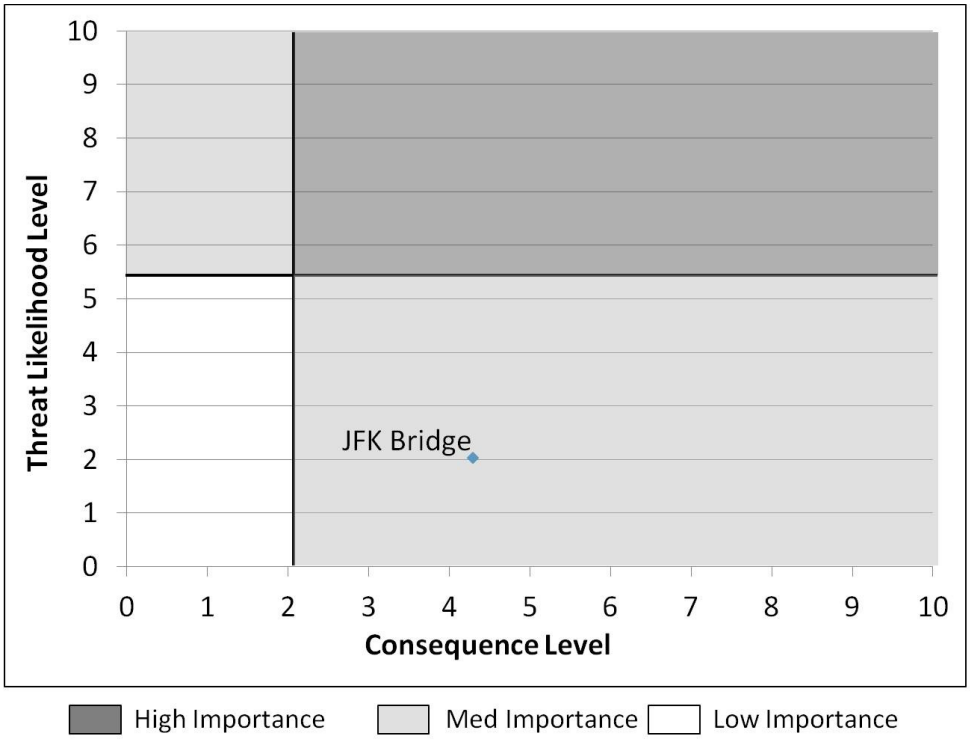
average factor levels of all the bridges in Indiana shown as the borders between colors (Figure 4.5.).



(a)JFK Bridge Threat Likelihood-Resilience Nomograph



(b) JFK Bridge Consequence-Resilience Nomograph



(c) JFK Bridge Threat Likelihood-Consequence Nomograph

Figure 4.5. Security Factor Levels of JFK Bridge

4.4. Security Rating

Based on the security factor outputs for the JFK Bridge using the given data, a security rating can be calculated in Equation 53 below. The overall security rating for the JFK Bridge is 1.31, a security rating of high importance as seen on the scale in Figure 4.5. A security rating of high importance indicates that unexpected failure can be avoided if an agency takes immediate action to enhance the resilience of the bridge and thus reduce the possible consequences. The JFK Bridge would therefore need improvements to increase its security rating and should be monitored to improve its secure standing.

$$SR_{JFK} = \frac{9.13^1}{(2.67^1+4.29^1)} = 1.31 \tag{53}$$

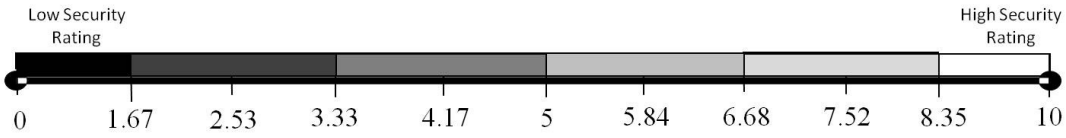


Figure 4.6. Security Rating Scale

Table 4.14. Interpretation of Security Rating

Security Rating	Example Interpretation
≤1.67	Indicates very high security improvement needs and low resilience thus immediate action should be undertaken to enhance resilience and thus reduce the possible consequences.
1.67-3.33	Indicates high security improvement needs of the asset. The agency should be ready to undertake actions to enhance resilience and thus to reduce the possible consequences of the asset failing.
3.33-5.00	Indicates medium-to-high security improvement needs. Facilities within this range can be monitored at a frequency slightly exceeding standard frequency. The risk of failure can be tolerated until a normal capital project (to enhance resilience and thus reduce consequences, among other benefits) is carried out.
5.00-6.68	Indicates low-to-medium security improvement needs. Unexpected failure can be avoided during the remaining service life of the asset by performing standard scheduled inspections with due attention to specific design features that influence the assets possible consequences.
6.68-8.35	Indicates low security improvement need. Often reflective of the likelihood of threat to a civil engineering system built to the current design standards in a low threat likelihood environment.
8.35-10	Indicates little or no security improvement needs.

4.5. Chapter Summary

This chapter presented an asset-level methodology to quantify the overall security rating for the JFK Bridge, in terms of the: threat likelihood, system resilience, and consequences in the event of system destruction or damage due to earthquake occurrence. The methodology addresses the risk measurement aspect of the traditional risk management framework. The next chapter applies the methodology to the Indiana bridge network to demonstrate how network-level security analysis will help decision-makers prioritize assets for risk management

CHAPTER 5: NETWORK LEVEL CASE STUDY

5.1. Introduction

This chapter applies the methodology developed in this dissertation to a transportation network. The Indiana state bridge network was used for the network-level case study along with earthquake threat information. The methodology is applied to each individual bridge to ascertain the security trends of the system. This analysis will help identify areas of security concern based on the three relevant security factors and spatial analysis of bridge security ratings. The security ratings of specific groups of bridges will determine if certain bridge characteristics play a significant role in asset security.

5.2. Data

The data compiled to demonstrate the methodology was from the Federal Highway Administration National Bridge Inventory (NBI) for the state of Indiana. The data collected for highway bridges included; the year of construction, total deck width, bridge length, superstructure material type, design type, condition, county location, average daily travel (ADT), roadways or waterways under a bridge, and detour length. Additional data included the number of earthquake epicenters in a county, county population data, county precipitation, county freeze index, construction cost, construction

time, replacement cost and asset value. Data for each specific security factor are listed in Table 5.1.

Table 5.1. Data Needs, Security Factors for Security Rating

Factors	Data Needs
Threat Likelihood	Natural Hazards Freeze Index Precipitation Environmental Barriers (waterways) Physical Barriers (roadways, railroad)
Resilience	Condition Age Construction Time Construction Cost Asset Size Material Design Type
Consequences	Population ADT Replacement Cost Value Detour Length Travel Time Increase from Detour

The data for natural hazards (earthquake epicenters) and county populations in Indiana was located in the IndianaMAP geographic information system (GIS) map database (IGS, 2014). Freeze index and precipitation data for Indiana was located in the National Oceanic and Atmospheric Administration (NOAA) database. Bridge replacement costs, values and construction costs were used from a study done on asset valuation in the state of Indiana (Dojutrek et al., 2012). The Elemental Decomposition and Multi-criteria (EDMC) valuation method was utilized to find the values of all bridges in the state of Indiana (Dojutrek et al., 2014). Table 5.2. presents the cost models used for bridge component replacement costs (Rodriguez et al., 2006). Construction time was

assumed to be related to construction cost, and travel time increase was assumed to relate to detour length and a travel speed of 45 miles per hour.

Table 5.2. Bridge Cost Data for the Case Study

Bridge Material Type	Bridge Component	Component Cost Models	Average Cost ($/sq.ft.)
Concrete Slab Bridges	Superstructure	$SUPC = (.2598 + .066 * PRESTRESSED) * BL^{.8122} * TDW^{.7223}$	$74.28
	Substructure	$SUBC = 1.2603 * BL^{.1124} * SUBH^{.767}$	$250.60
	Approach	$APPC = 53.6713 + .1970 * ADT$	N/A
	Other	$OTHC = .856 * BL^{.955} * TDW^{.2995}$	$91.93
Concrete Beam Bridges	Superstructure	$SUPC = .0244 * BL^{1.0879} * TDW^{1.0424}$	$64.55
	Substructure	$SUBC = -37.848 + .023 * DA$	$134.43
	Approach	$APPC = -772 + .563 * BL + 19.05 * TDW + 18.71 * SUBH$	N/A
	Other	$OTHC = .0422 * BL^{.4283} * TDW^{1.3412} * SUBH^{.6577}$	$0.30
Steel Bridges	Superstructure	$56.66/sq.ft.	
	Substructure	$17.12/sq.ft.	
	Approach	$56.36/sq.ft.	
	Other	$45.12/sq.ft.	

Source: Rodriguez et al. 2006

Where *SUPC* is the total superstructure replacement cost for bridges (1,000's 2002$); *BL* is the bridge length (ft.); *TDW* is the total deck width (ft.); *PRESTRESSED* holds a value of 1 if the superstructure made of prestressed concrete, 0 otherwise; *SUBC* is the total substructure replacement cost (1,000's 2002$); *SUBH* is the substructure height (ft.); *APPC* is the total approach replacement cost (1,000's 2002$); *ADT* is the average daily traffic; *OTHC* contains the costs related to traffic control, excavation, mobilization, demobilization, and office expenses (1,000's 2002$); and *DA* is the deck area (sq.ft.).

5.3. Network Level Security Rating Analysis

The security rating method was applied to each bridge in the state of Indiana at the asset-level using the data described above. Distributions of each security factor for the Indiana bridge network can be seen in Figures 5.1.-5.3.

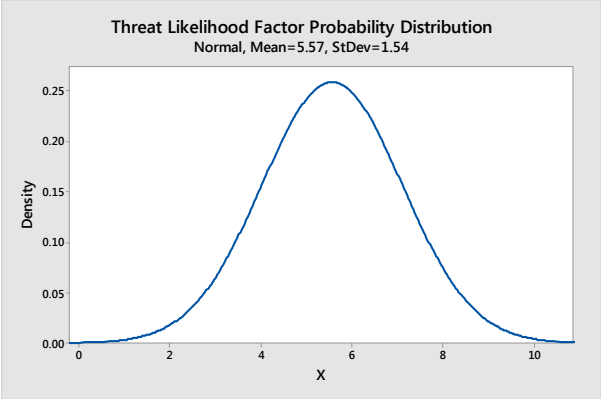


Figure 5.1. Indiana Bridge Network Level Distribution of Threat Likelihood Factor

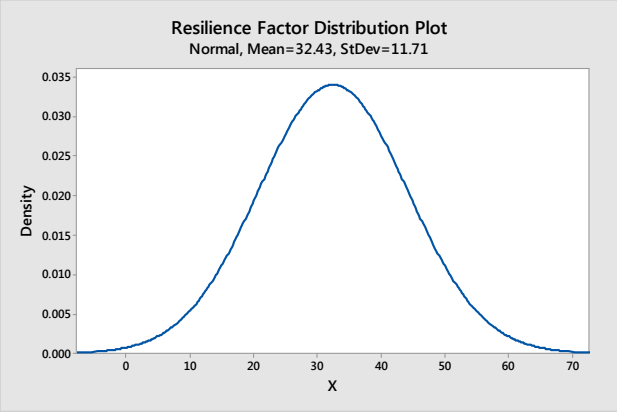


Figure 5.2. Indiana Bridge Network Level Distribution of Resilience Factor

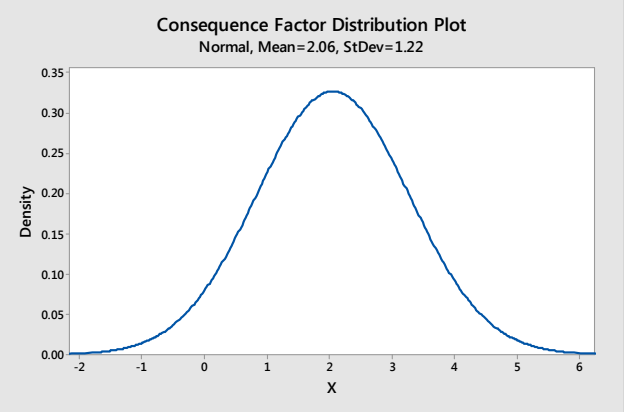


Figure 5.3. Indiana Bridge Network Level Distribution of Consequence Factor

The security rating histogram of all bridges in the state of Indiana is visualized in Figure 5.4. Many of Indiana's bridges have a low-to-medium security rating with some bridges in the very low security rating range. The bridges with low security ratings may be of interest to decision-makers when allocating resources.

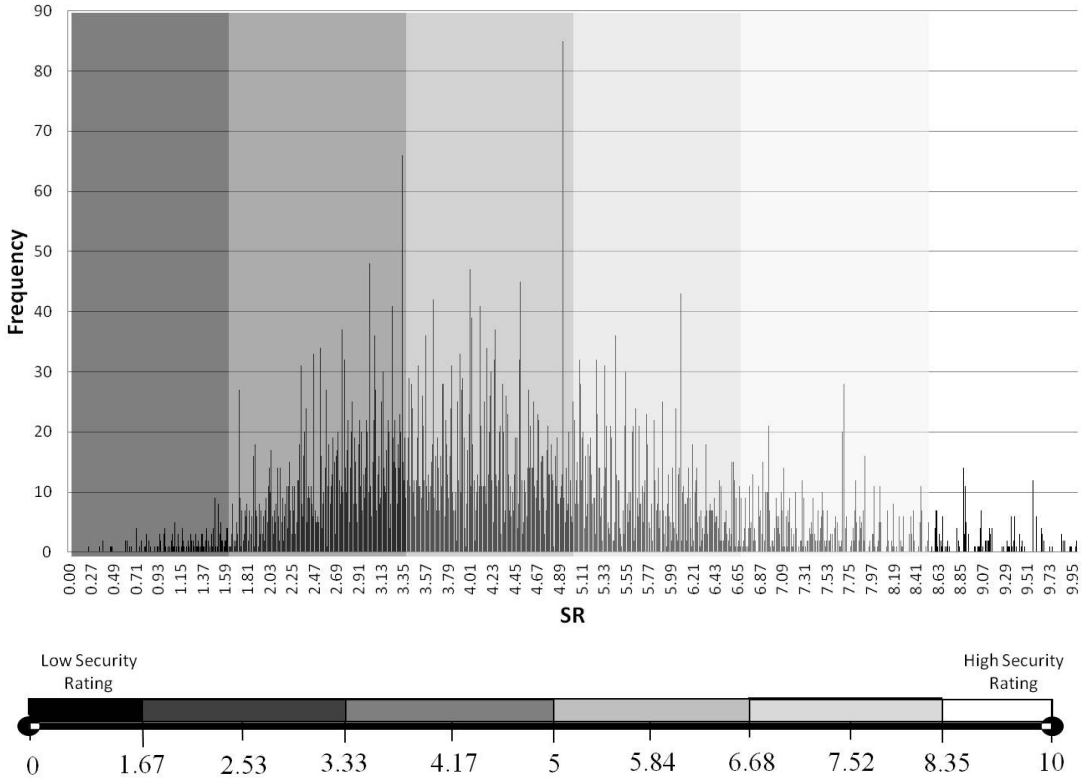


Figure 5.4. Indiana Bridge Network Level Histogram of Security Rating

Security ratings for Indiana's bridge network were calculated and the factors for each bridge were graphed in different combinations (Figures 5.5-5.7.). Of the total number of bridges in Indiana, 2.34% of the bridges have low security ratings (1.67<SR), 62.91% of the bridges have low-to-medium security ratings (1.67<SR<5.0), 30.77% of the bridges have medium-to-high security ratings (5.0<SR<8.35), and 3.99% of Indiana bridges have high security ratings (SR>8.35).

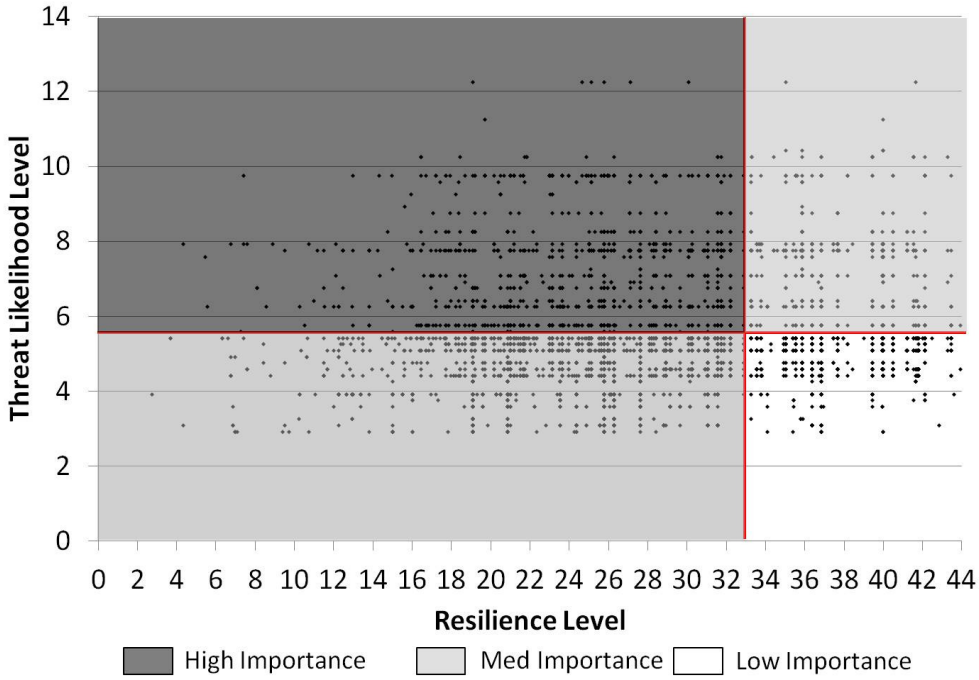


Figure 5.5. Indiana Bridge Network Threat Likelihood-Resilience Nomograph

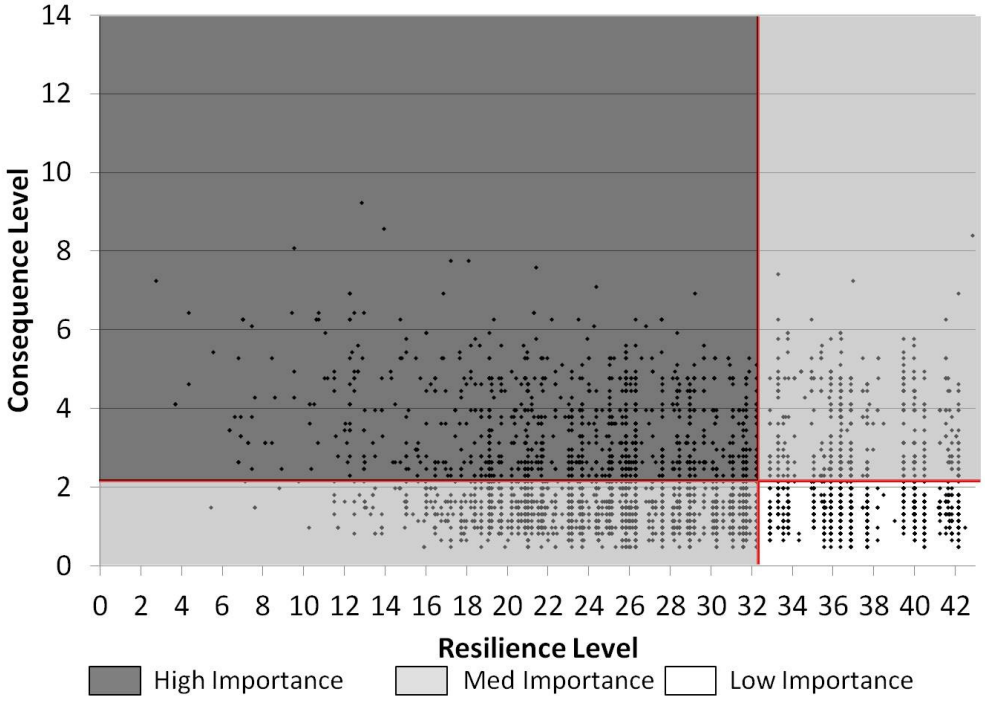


Figure 5.6. Indiana Bridge Network Consequence-Resilience Nomograph

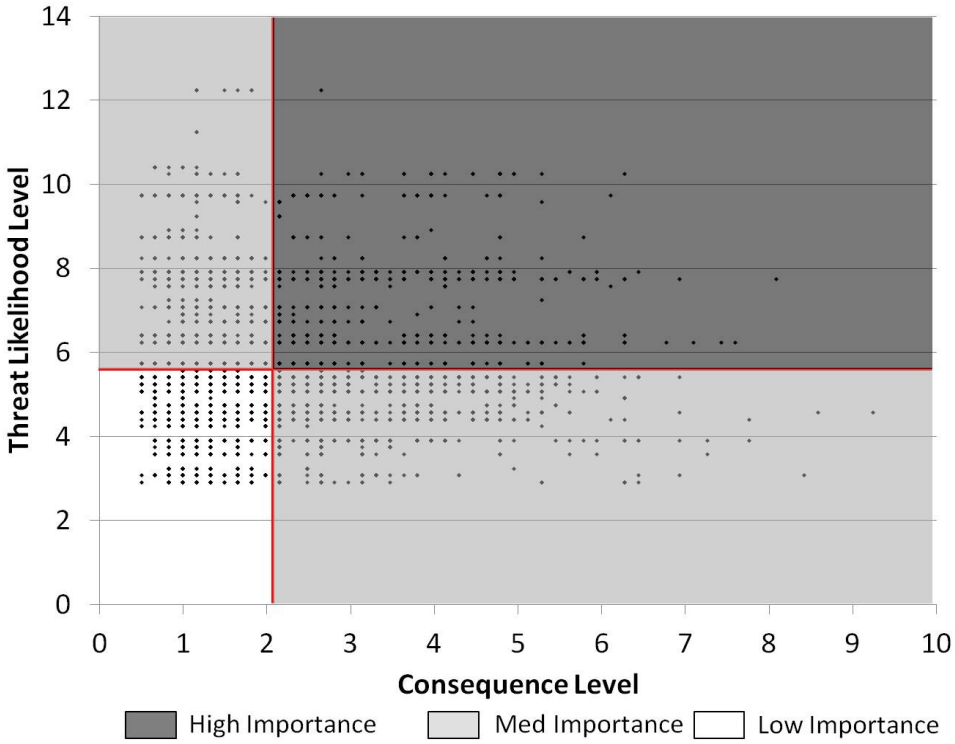


Figure 5.7. Indiana Bridge Network Threat Likelihood-Consequence Nomograph

As demonstrated in the figures, many of Indiana's bridges lie in the high importance (dark gray) regions. Further analysis was conducted by organizing the Indiana bridge network by material type, geographic region, route type, and NHS status. To normalize each category, the frequency of each security rating was divided by the total number of bridges in each category. The normalized frequency numbers were presented as percentages. For example, in Figure 5.8., there are a higher percentage of urban bridges with a security rating of 5.0 than rural bridges. The scale in Figure 5.4. is based on Indiana network security ratings with a mid-range rating of 5.0. If a security rating of 1.67 is the cutoff for assets that require large improvements to increase their security, further conclusions can be made.

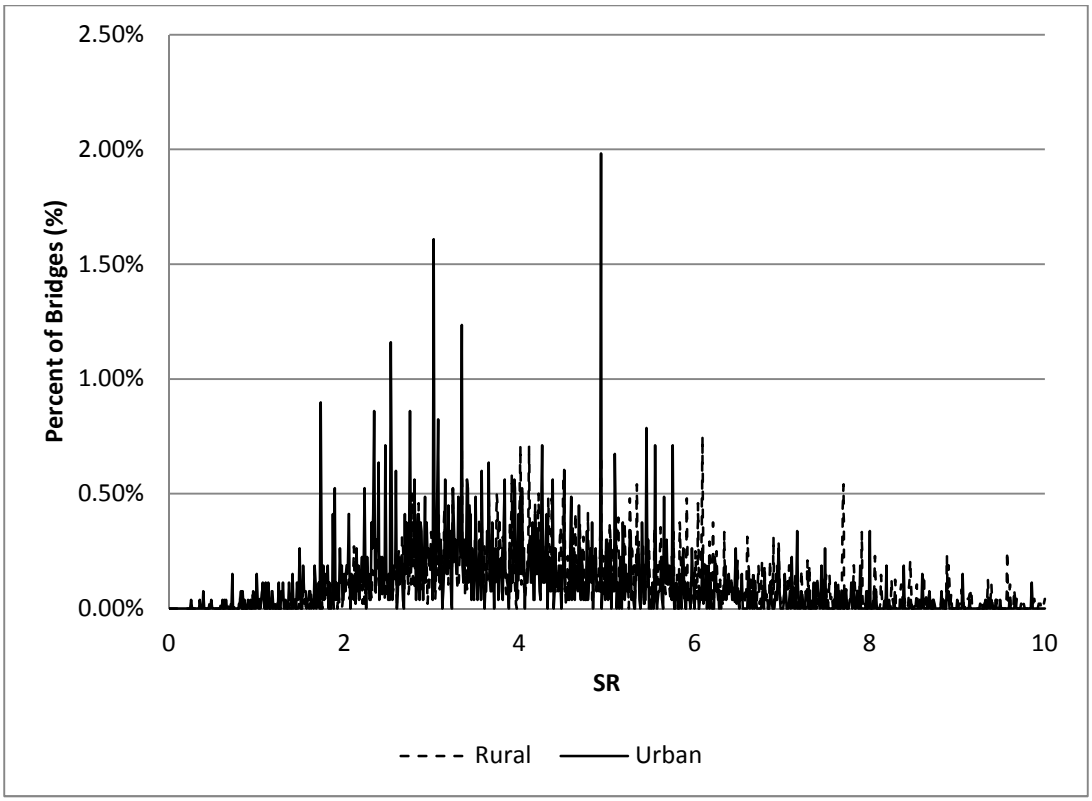


Figure 5.8. Security Rating of Bridges by Geographic Region.

The percentage of rural bridges with a security rating below 1.67 is 1.42% while urban bridges have 4.12% below this rating (Figure 5.8.). This implies that urban bridges have increased design standards for large traffic volumes and may receive a greater frequency of maintenance due to wear and tear. Rural bridges may have lower design standards due to low traffic volumes and may require less frequent maintenance cycles due to less traffic wear and tear. More frequent maintenance may increase asset conditions over time, which contributes to higher resilience and higher security ratings.

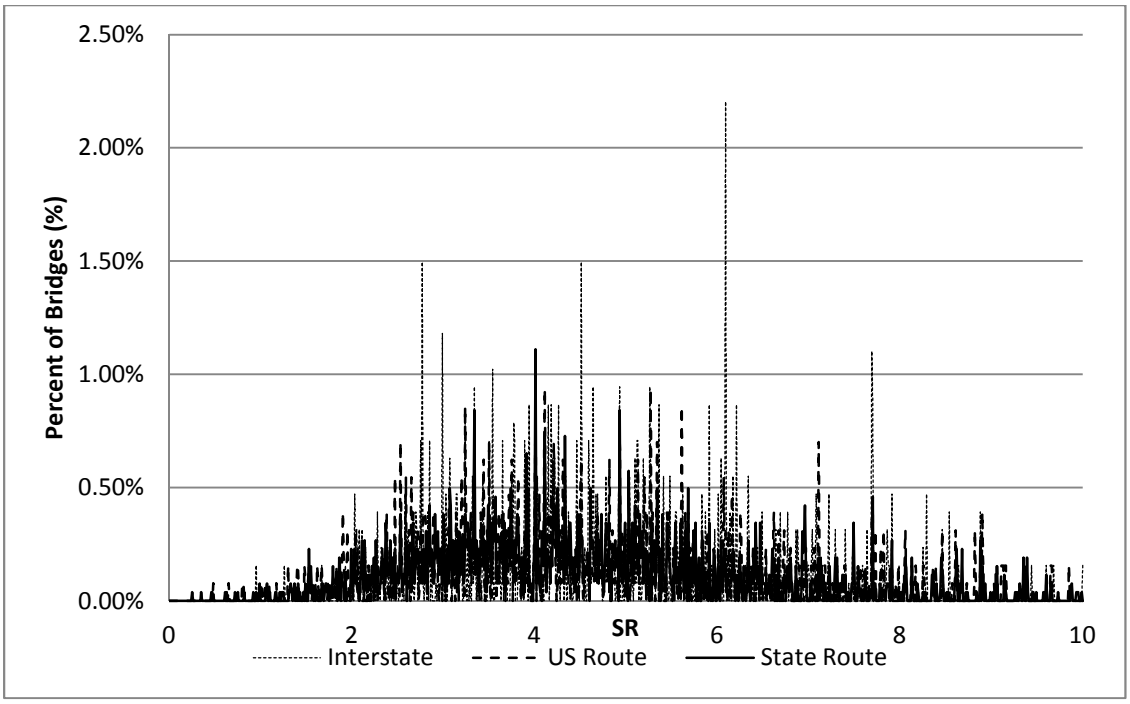


Figure 5.9. Security Rating of Bridges by Route Type

Interstate, U.S. route, and state route bridges had percentages of 0.55%, 2.42%, and 2.15% of their bridges below a security rating of 1.67 (Figure 5.9.). This implies that Interstate bridges have higher design standards (e.g., thicker pavement) which play a role in increasing security ratings while U.S. route and state route bridges have different or less stringent design standards compared to interstate bridges. By combining geographical location and bridge type (Figure 5.10.), 0.55% of rural interstate bridges are below the 1.67 security rating and 5.39% of urban interstate bridges. This implies that interstate bridges located in an urban location may have higher design standards, but the consequences of failure are greater than in a rural location. More people are located in urban areas to travel over the bridges and may be affected if the bridge was closed due to increased travel times on detours and possible injuries.

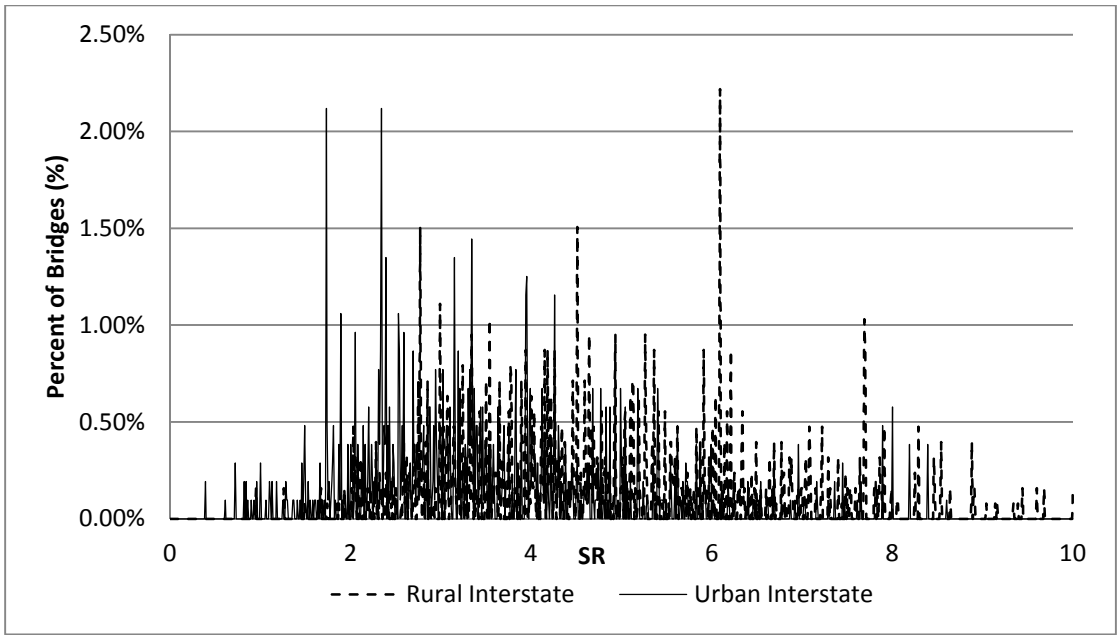


Figure 5.10. Security Rating of Interstate Bridges by Geographic Region

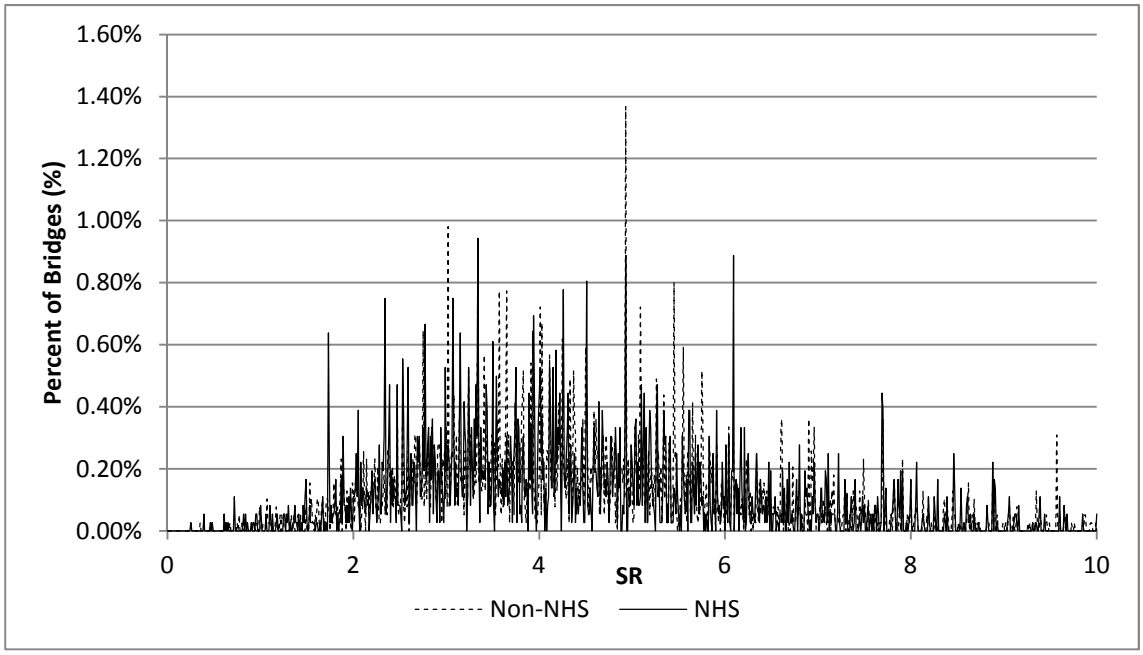


Figure 5.11. Security Rating of Bridges by NHS Status

Non-NHS (National Highway System) bridges had 2.17% of bridges below a security rating of 1.67 and NHS bridges had 2.64% below this rating (Figure 5.11.). This

can result from higher traffic volumes on NHS roads and therefore greater consequences from travel time increases and possible injuries if the bridge fails. Non-NHS roads may be are locally managed and may not be held to the standards indicated for NHS roadways, but may be less traveled. These characteristics may lead to the differences in total percentage of bridges below the 1.67 security rating threshold.

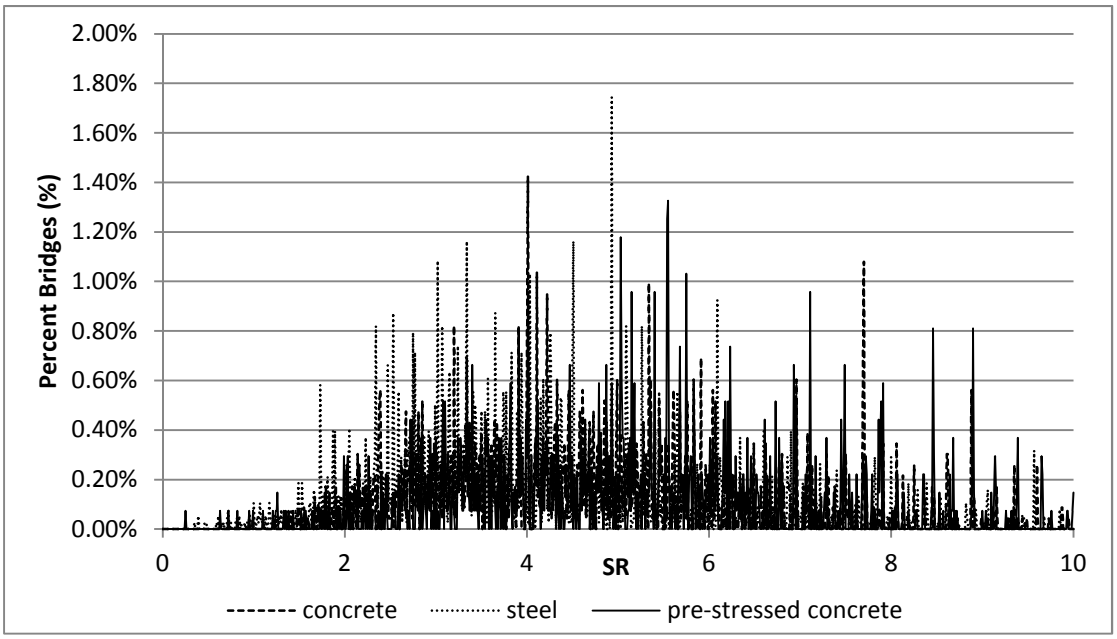


Figure 5.12. Security Rating of Bridges by Material Type

Steel, concrete, and pre-stressed concrete bridges had 3.73%, 0.69%, and 1.55% of their total bridges below the 1.67 security rating. This implies that concrete bridges may be more secure than steel bridges, but could be due to geographic location. Steel bridges may be located in more urban areas while concrete bridges could be located in rural areas. Additionally, different bridge types may have been preferred over others in past construction practices therefore leading to the differences. These characteristics could play a role in influencing the security ratings of these bridges.

5.3.1. Spatial Analysis

Further modeling techniques should be conducted to examine the security rating and infrastructure characteristics interaction through GIS ArcMap 10.1 for spatial analysis. As seen in Figure 5.13., many bridges around Indianapolis, Indiana have a low security rating. Indianapolis is in an urban location with a high population density. Many bridges leading into the city are highly traveled and, if closed, can cause large traffic delays. Therefore, these characteristics can play a large role in the low security ratings of these bridges. Additionally, many bridges located in the outer perimeter of Indianapolis have a higher security rating, implying that these bridges may be less traveled and located outside the urban area. From an agency perspective, spatial analysis provides the means to pinpoint low security areas where improvements should be focused. Spatial analysis would help identify areas of high consequences in the case that a bridge did fail. In Figure 5.13., this area is located in the heart of the city.

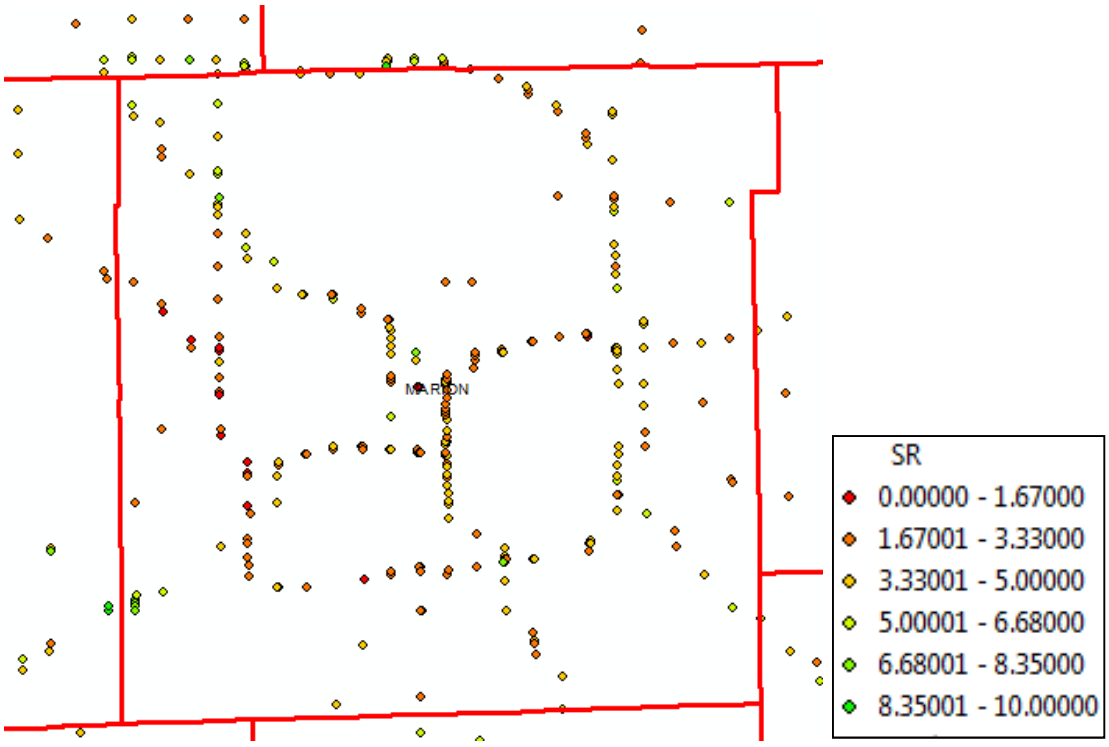


Figure 5.13. Visualization of Indianapolis Bridges using Security Rating

5.4. Chapter Summary

By analyzing transportation infrastructure from a network-level perspective, specific infrastructure types with low security ratings are identified. The characteristics that lead to low security ratings are able to be cataloged for future reference. Spatial analysis further enables agencies and stakeholders to visualize areas of concern and work to secure the infrastructure in those locations. This case study is an example of analyzing infrastructure at the network level based solely on security. Chapter 6 further describes how uncertainty is incorporated into the security rating framework.

CHAPTER 6: INCORPORATION OF UNCERTAINTY IN INFRASTRUCTURE SECURITY ASSESSMENT

6.1. Introduction

In view of their inherently dynamic and highly unpredictable nature, threat likelihood, infrastructure resilience, and consequence are difficult to determine with certainty. Due to this problem, this chapter enhances the basic framework presented in the previous chapter using fuzzy logic techniques. The method is particularly useful when data is unavailable or imprecise, allowing the security rating to be determined using a qualitative expert-assigned level with each factor contributing to overall security. The evaluation of the security factors are represented as fuzzy triangular numbers with accompanying membership rules that define the extent of contribution by each factor to overall infrastructure security. Then, using a case study, the chapter applies the fuzzy-based methodology to illustrate how uncertainty considerations could be included in determining the overall security of specific infrastructure.

6.2. Uncertainty

Uncertainty causes encompass a wide range including: lack of information, an abundance of information (complexity), conflicting evidence, ambiguity, measurement, etc. Uncertainty due to ambiguity includes (i) physical randomness, (ii) statistical

uncertainty due to limited information in estimation and the characteristics of these variables, and (iii) model uncertainty due to simplifying assumptions in analytical models, predicative models, simplified methods, and idealized representations of real performances (Ayyub and Gupta, 1997). Uncertainty due to vagueness is caused by (i) variable definitions, (ii) human error and factors, and (iii) defining interrelationships among problems variables (Ayyub, 1992). Information can also vary from set numerical data to rough linguistic opinion, which in turn determines the quality and quantity of available data. In this dissertation, uncertainty is defined as "a human-related subjective notion which depends on the quantity and quality of information which is available to a decision-maker about a system of its behavior that the decision-maker wants to describe, predict, or prescribe." This is the same manner in which uncertainty is identified by Ayyub and Gupta (1997).

Threat likelihood is very uncertain due to the nature of natural and man-made threats. It is difficult to predict with certainty the exact moment transportation infrastructure is likely to fail due to the complexity of both internal and outside forces. For example, a bridge may be located near an earthquake fault, but it may have been dormant for many years. In this instance, a sudden catastrophic tremor may occur seemingly without warning. Similarly, if infrastructure is built with faulty material or a design flaw, the infrastructure may not be affected until the component fails, often without notice. Accidents and threats of both natural and man-made variety cannot be predicted with 100% accuracy due to their inherently uncertain nature.

Consequences are also highly variable and not easily predicted. For example, a component of a bridge may fail, but the bridge may still appear to be structurally sound

before the problem is found. In another case, an important component failing may lead the entire bridge to succumb. Additionally, the consequences due to a bridge closure may affect users and agencies differently. A user may have increased travel time due to re-routing to another bridge to get across a river, while an agency would need to find additional funds to repair a damaged bridge. The uncertain nature of infrastructure damage and its consequences lead to ambiguity in predicting them.

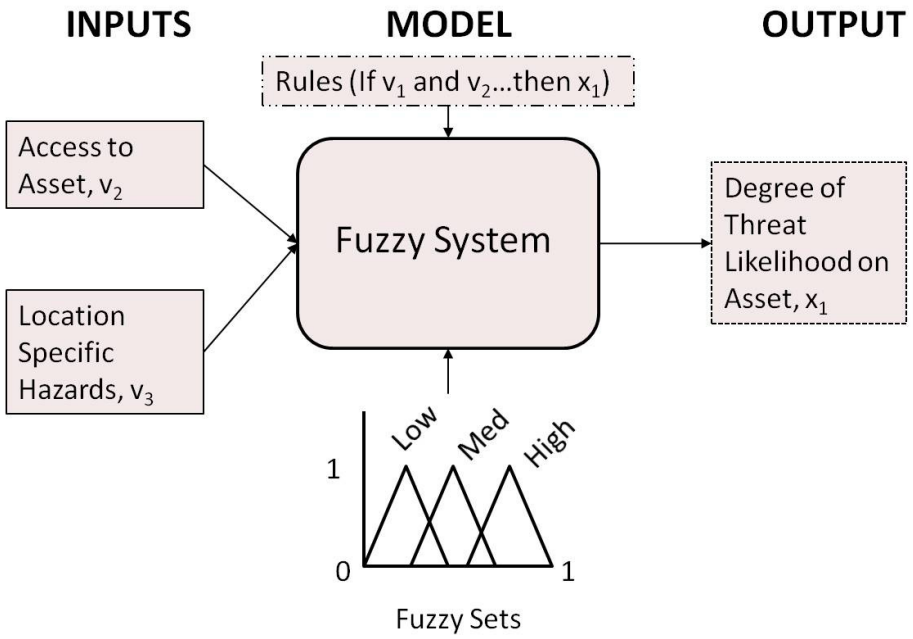
Resilience is also uncertain in nature because infrastructure can be designed and built to be resilient, but a mistake in the drawings or construction can lead to failure during a threat occurrence. Uncertainty must be accounted for when security of infrastructure is being explored.

6.3. Fuzzy Logic Framework

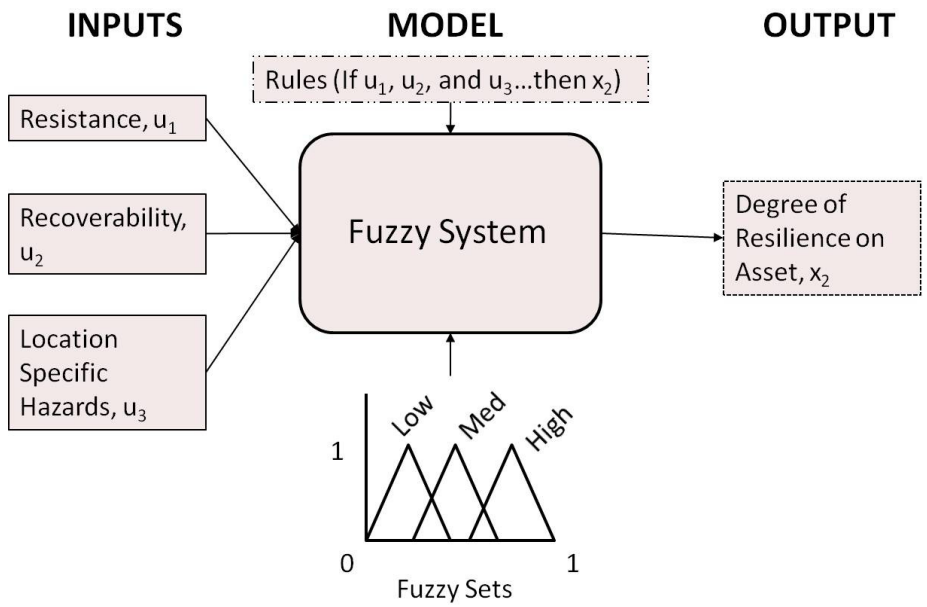
As previously stated, the security of an infrastructure is a function of three main factors: (1) the threat likelihood, (2) infrastructure resilience, and (3) consequence. The security rating metric developed in Chapter 3 combines these factors. This chapter duly accommodates the fact that all three factors are characterized by a significant degree of uncertainty; and therefore, introduces fuzziness in the levels of these factors and in their outcome (e.g., the security rating). The enhancements to this method will allow experts to use the security rating method in situations where they are faced with imprecise or inadequate data.

A fuzzy logic framework for fuzzification of the security-related measures and attributes is particularly useful when decision makers lack access to infrastructure-

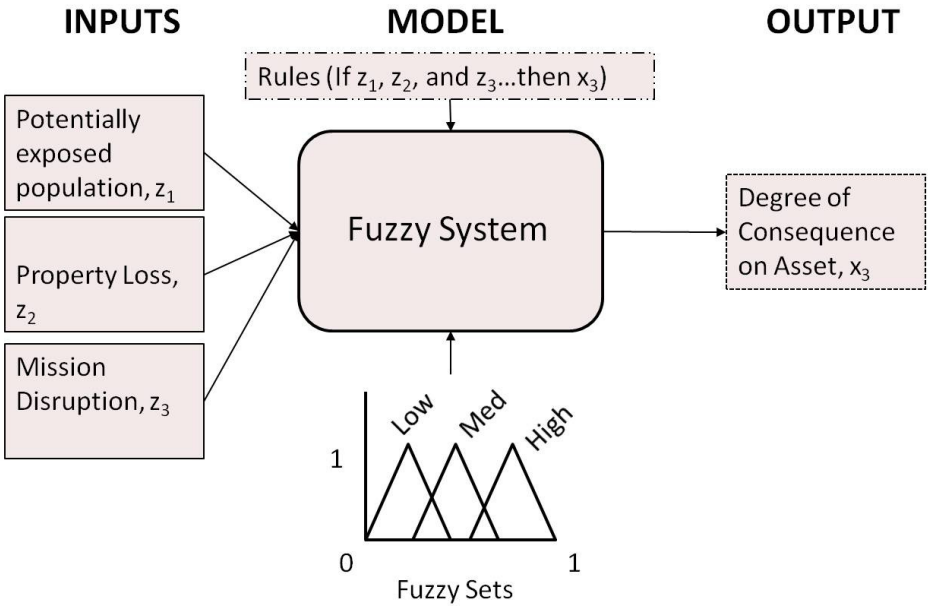
specific information for each factor. The framework inputs fuzzy data into the security rating equation to yield a fuzzy output. The Matlab Fuzzy Toolbox (MathWorks, 2013) was used to program this framework. For example, each factor can be fuzzified to output a level of that specific factor as seen for the threat likelihood factor (Figure 6.2.) (Dojutrek, et al, 2014). Each measure has a "degree of membership" ranging from low to high on a pre-specified scale. The value of the factor depends on the level of each measure, and the measure levels are in turn determined by their respective consistent attributes. The value of each fuzzified factor is then input into the overall security rating fuzzy-based analysis that yields a fuzzy security rating for a specific infrastructure (Figure 6.1.).



(a) Threat Likelihood Factor

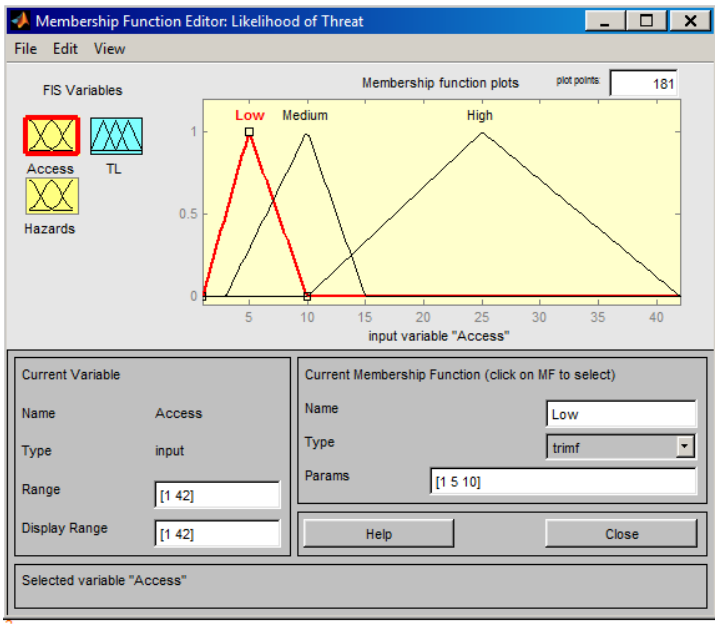


(b) Resilience Factor

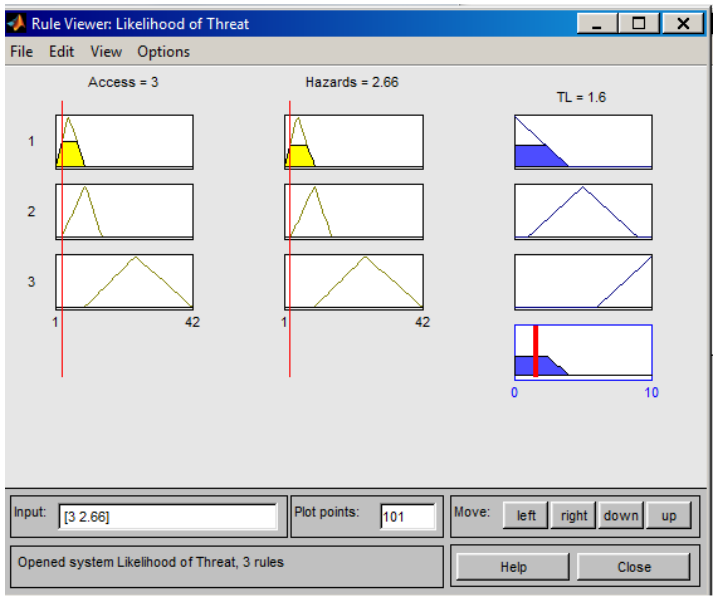


(c) Consequence Factor

Figure 6.1. Fuzzy Logic Models for the Factors of Infrastructure Security Rating.



(a) Threat Likelihood Membership Functions



(b) Fuzzy Threat Likelihood Model

Figure 6.2. Fuzzy Threat Likelihood Factor and Attributes.

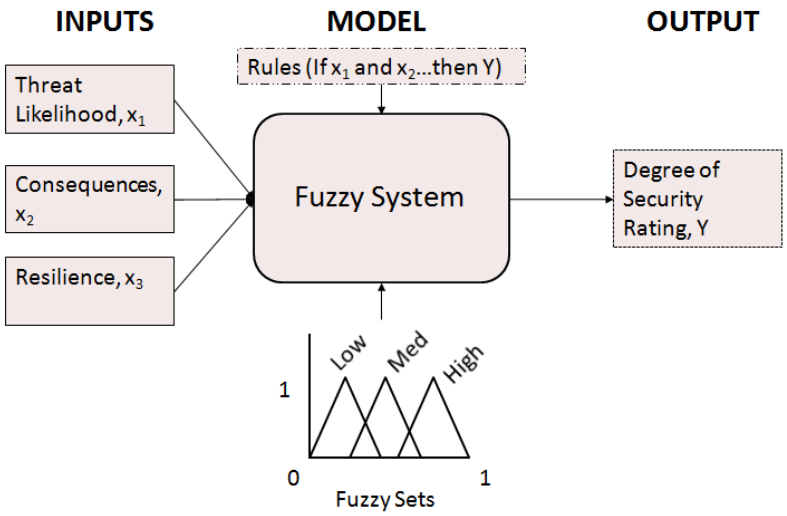


Figure 6.3. Fuzzy Security Rating.

6.4. Rules

Fuzzy rules were developed to determine the fuzzy security rating output for the fuzzy logic system. The rules give mathematical meaning to the different linguistic levels of each factor in the security rating framework (Figure 6.4.). Thus, a complete fuzzy inference system is created. Fuzzy membership functions for the security rating are shown in Figure 6.4.

Rules:
If *resilience* is high, *consequence* is low, and *threat likelihood* is low, then *SR* is high.
If *resilience* is high, *consequence* is high, and *threat likelihood* is high, then *SR* is medium.
If *resilience* is high, *consequence* is medium, and *threat likelihood* is medium, then *SR* is medium.
If *resilience* is medium, *consequence* is medium, and *threat likelihood* is medium, then *SR* is medium.
If *resilience* is medium, *consequence* is low, and *threat likelihood* is low, then *SR* is medium.
If *resilience* is medium, *consequence* is high, and *threat likelihood* is high, then *SR* is low.
If *resilience* is low, *consequence* is medium, and *threat likelihood* is medium, then *SR* is low.

If *resilience* is low, *consequence* is high, and *threat likelihood* is high, then *SR* is low.
If *resilience* is low, *consequence* is low, and *threat likelihood* is low, then *SR* is medium.

		Threat Likelihood								
		Low			Medium			High		
		Consequence			Consequence			Consequence		
		L	M	H	L	M	H	L	M	H
Resilience	Low									
	Medium									
	High									

Low SR Medium SR High SR

Figure 6.4. Visualization of Fuzzy Rules.

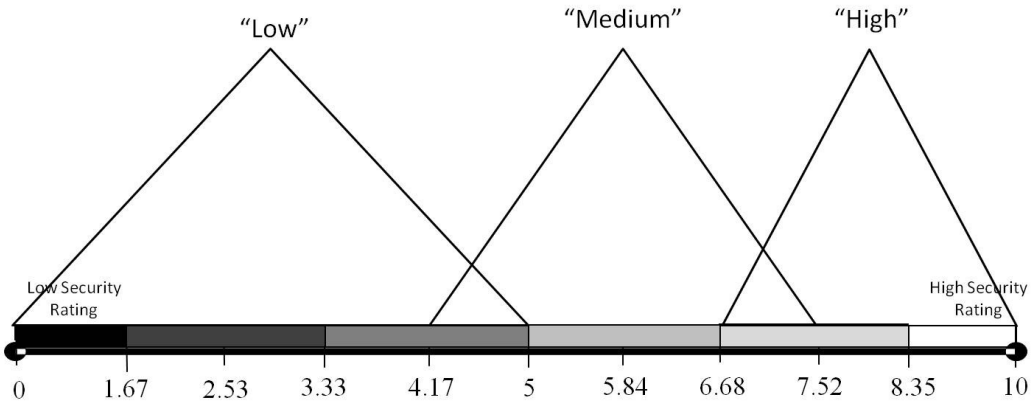


Figure 6.5. Fuzzy Membership Functions.

6.5. Case Study for Fuzzy Security Rating

To demonstrate the framework developed for fuzzifying the security ratio, the Leo Figo Memorial Bridge in Green Bay, Wisconsin, National Bridge Inventory (NBI) structure number B05015800100000, was used (Figure 6.6.). Data was collected from the

National Bridge Inventory (FHWAb, 2014). The factors, measures, and attributes used for the case study are described in Figure 6.7.

Figure 6.6. Leo Frigo Memorial Bridge, Green Bay, Wisconsin.

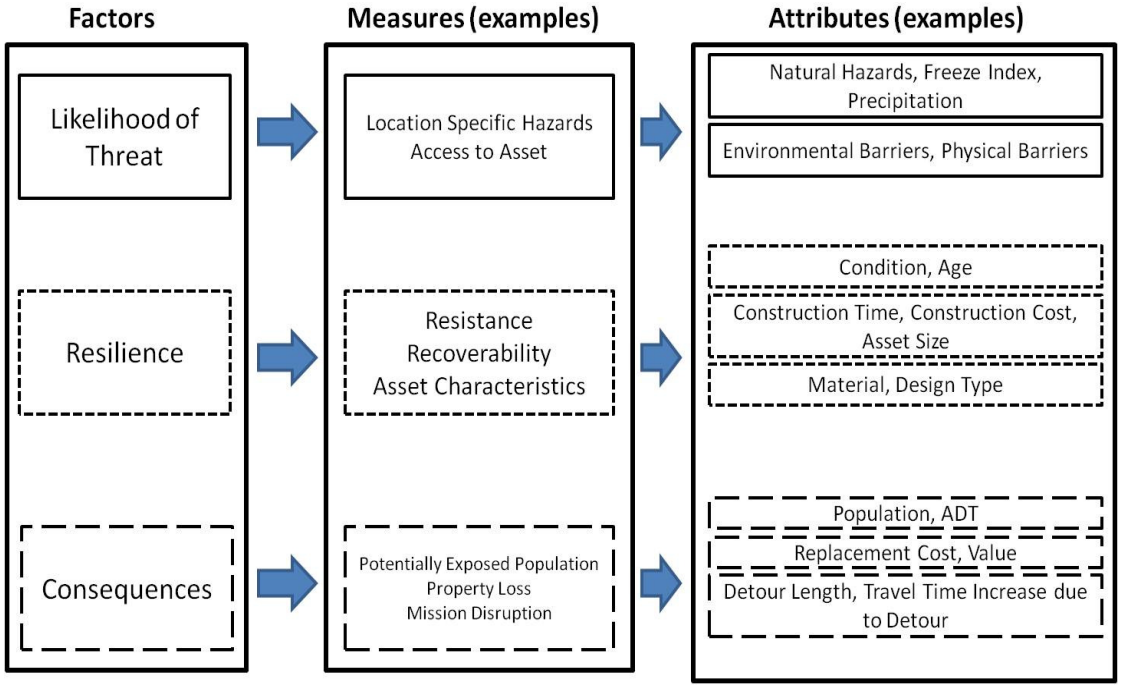


Figure 6.7. Detailed Framework for Case Study (Dojutrek et al, 2014).

A number of assumptions were made for this case study. First, the construction time (days) was based on the bridge size (ft^2). Second, environmental barriers were assumed to be the waterway under the bridge. The detour travel speed was assumed to be 45mph, and all weights in the security rating equation (α, δ, λ) and measures equation were assumed to be equal. Threat likelihood measures, attributes, and scales can be seen in Table 6.1. This data was taken from the NBI database. The result of each measure is the scaled attributes multiplied together and normalized by the number of attributes for each measure, and then subsequently multiplied by the measure's weight. An uncertainty-based expression of the degree of the threat likelihood, asset resilience, and consequence is established after these results are analyzed. The fuzzy degree of threat likelihood is 1.6, the fuzzy degree of resilience is 5.0, and the fuzzy degree of consequence is 1.78.

Table 6.1. LFM Bridge Factor Data.

Threat Likelihood				
Access to Asset	Environmental Barriers	Over Fox River	3	3
	Physical Barriers	Independent bridge protection	2	
Location Specific Hazards	Natural Hazards	High winds, fog	4	2.66
	County Freeze Index	189.3	2	
	County Precipitation	29.52	1	
Resilience				
Resistance	Condition	Deck: 8	5	50
		Superstructure: 7	5	
		Substructure: 6	4	
	Age	35 yrs	2	
Recoverability	Const. Time	3yrs	3	9
	Const. Cost	$6.85M	3	
	Asset Size	39,115 ft^2	3	
Asset Characteristics	Material	Steel	4	2
	Design Type	Thru-Arch	1	
Consequence				
Potentially Exposed Population	Population	Green Bay: 104,868 Brown County: 253,032	4	6
	AADT	31,400	3	
Property Loss	Replacement Cost	$6.92M	3	3
	EDMC Value	$4.34M	2	
Mission Disruption	Detour Length (miles)	~6 miles	2	4
	Inc. in travel time due to detour	8 min	4	

The fuzzy degree of each security factor, (threat likelihood, resilience, and consequence), are input into the fuzzy security rating framework (Figure 6.8.), which results in an overall fuzzy security rating of 5.84 for the Leo Frigo Memorial Bridge. This rating corresponds to a security rating of “medium” as shown in Figure 6.5.

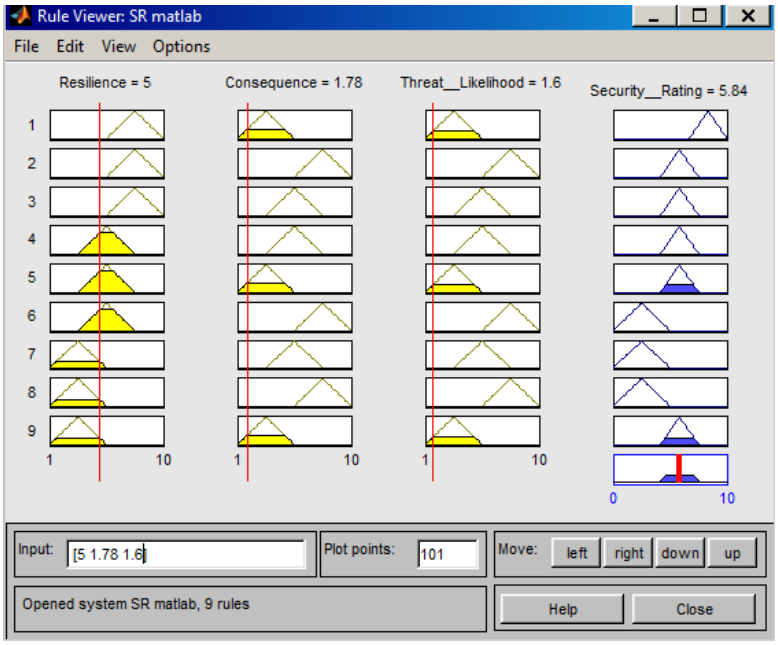


Figure 6.8. Overall Fuzzy Security Rating.

6.6. Monte Carlo Simulation

A technique is needed to examine how variations in the security factors for a specific infrastructure influence the resulting security rating, given a normal distribution of each factor based on the average and standard deviation of all the security factors. For this, the Monte Carlo simulation was used. The Monte Carlo simulation is a computerized mathematical technique that allows people to account for variability in their process to enhance quantitative analysis and decision making (Palisade Co., 2014). The simulation works by analyzing models of a range of possible values and results (probability distributions) for any factor that has inherent uncertainty. The simulation establishes the outcome of thousands of scenarios each using a different set of random values from the probability distributions. The results of the Monte Carlo simulation are the distributions of possible outcome values. A Monte Carlo simulation has a number of

advantages over deterministic analysis including: probabilistic results (what could happen and how likely each outcome is), graphical results; sensitivity analysis, scenario analysis (see which inputs had which values together when certain outcomes occurred), and correlation of inputs.

Figure 6.9. gives a visual representation of the Monte Carlo simulation procedure for the security rating. The probability distributions shown in the figure are only for illustration. Figure 6.10 was developed for the actual distributions. A total of 5,000 iterations were run for the simulation where the mean and standard deviation of the starting parameters (threat likelihood, resilience, and consequence) were derived from the Indiana NBI bridge database. Table 6.2. presents the statistics associated with the Monte Carlo simulation.

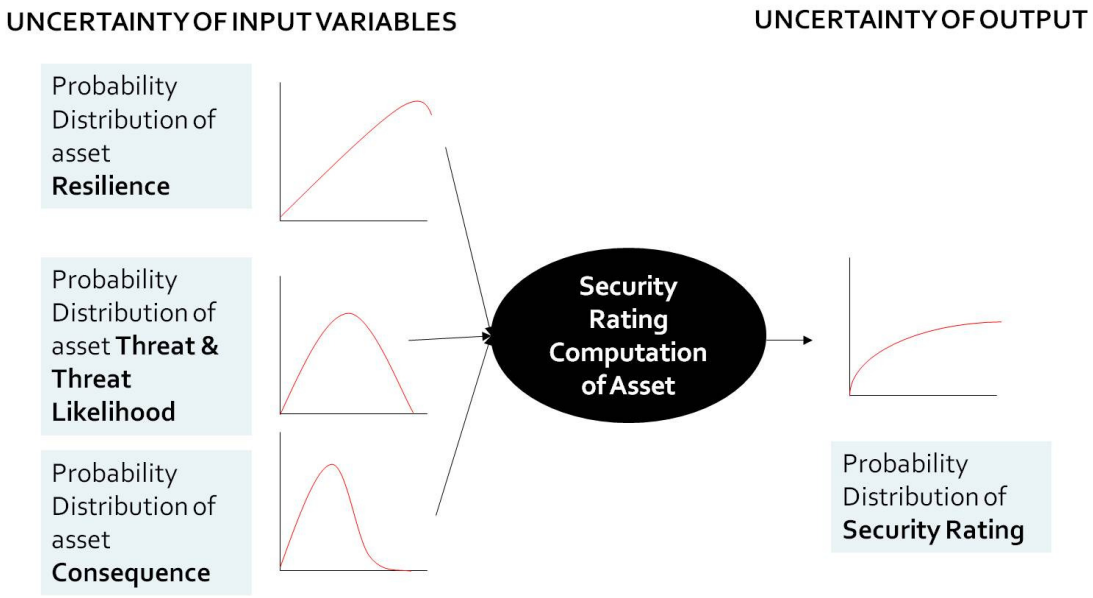
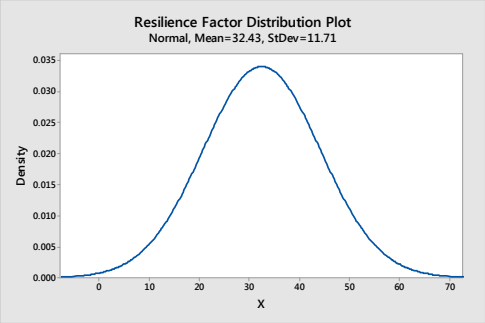
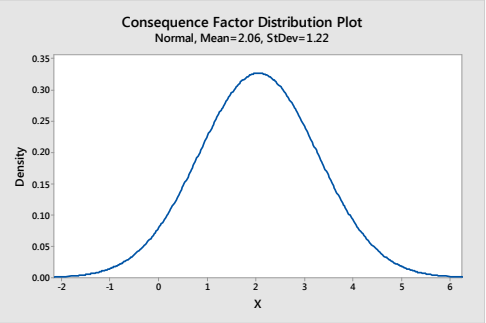


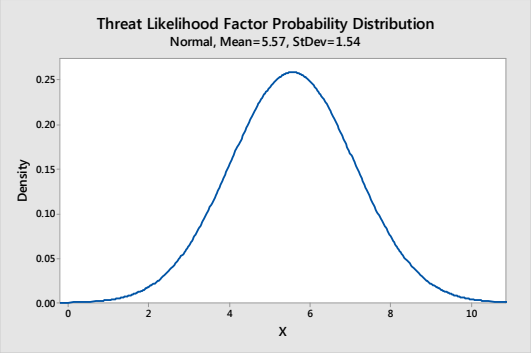
Figure 6.9. Monte Carlo Simulation of Security Rating.



(a) Resilience Factor



(b) Consequence Factor



(c) Threat Likelihood Factor

Figure 6.10. Distributions of Security Factors.

Table 6.2. Monte Carlo Simulation Probabilistic Security Rating

Statistics	Bridge
Total Simulation Runs	5,000
Sample Mean	5.653
Median	4.808
Sample Standard Deviation	3.477
Quartile (.75), Quartile (.25)	7.117, 3.326
Skewness	2.09
Kurtosis	8.10
Inter-quartile Range	3.791
Standard Error	0.049
95% Upper, Lower Confidence Level	5.749, 5.557
95% Central Interval Limits	1.522, 14.545

Kurtosis captures the steep or gradual slope of a distribution compared to the normal distribution. A positive kurtosis describes a relatively steep distribution. Negative

kurtosis indicates a relatively flat distribution. Skewness captures the degree of asymmetry of a distribution surrounding its mean. Positive skewness indicates that the tail of a distribution is asymmetric toward the positive values. Negative skewness indicates that the tail of a distribution is asymmetric toward the negative values. The mean security rating from the simulation is 5.653, indicating a "medium" security rating. The positive kurtosis indicates the distribution is relatively peaked at the mean; and the positive skewness indicates the tails of the distribution are asymmetrical, leaning towards higher security ratings. The quartile ranges indicate that most security ratings for the simulation are in the "medium" range for this bridge.

6.7. Chapter Summary and Discussion

Previous literature did not adequately consider the uncertain nature of threat likelihood, infrastructure resilience, and consequences in the event of threat occurrence. The information was largely qualitative in several other methodologies. A method that can transform such qualitative information into a quantitative form would be useful in overall security and ultimately in prioritizing infrastructure for transportation investment evaluation or security funding allocation.

This chapter first presented a framework to quantify the three factors of security using fuzzy logic. Each security factor was fuzzified using "high," "medium," and "low" levels of its respective measures and membership functions. The factors were input into the framework that provides the fuzzy security rating for specific infrastructure. A fuzzy

system captures the dynamic and uncertain nature of each security factor by creating a fuzzy set of numbers for each level of membership.

The Leo Frigo Memorial Bridge in Green Bay, Wisconsin was used as a case study for the fuzzy-based framework. Data was taken from the United States National Bridge Inventory database to use as an example for determining security measure levels and membership functions for each security factor. All the attribute values were scaled, and the respective measures fuzzified for input into the overall fuzzy security rating framework. The Leo Frigo Memorial Bridge was found to have a security rating of 5.84 which can be considered “medium.” The case study illustrated how the fuzzy security rating can account for the uncertain nature of the security-related data.

CHAPTER 7: USING SECURITY RATING IN INVESTMENT EVALUATION OR PRIORITIZATION

7.1. Introduction

Security is a performance criteria associated with little observable return on investment. This makes it difficult to balance security costs with other more traditional transportation agency initiatives such as economic efficiency, travel time, and/or safety (SAIC & PB Consult, 2009). Security initiatives must be well defined in order to successfully compete with other performance measures in the context of multi-criteria decision-making. This chapter creates a case for including security as a stand-alone performance measure and prioritizing projects based on their individual contributions to security improvement. Increase in security due to alternative improvements has the potential to influence decisions in a multi-criteria evaluation process.

7.2. Security Rating as a Performance Measure

Many considerations must be addressed when choosing evaluation criteria for security investments. In terms of security, effectiveness (benefits) can be captured in the resilience term. A highly resilient infrastructure will withstand damage from a hazard and reduce the consequences associated with total destruction of the asset. Security costs include the consequences due to infrastructure damage from a threat. Examples include

both agency costs (damage costs and repair costs) and user costs (travel time increase and detours). The impact on security due to an alternative improvement can be captured through the security rating. The cost effectiveness of an alternative investment can be measured in terms of the increase to the security rating or the security rating of an asset after implementation of the investment project. Figure 7.1. provides a depiction of the change in security rating over time for a given asset. When the asset is first constructed, the security rating is most likely to be high due to the fact that new construction more frequently adheres to modern building standards. Throughout the asset lifecycle, the security rating will decrease due to increased usage, general wear and tear, and ageing of the physical infrastructure (e.g., increased travel demand, environmental impacts, or obsolete building standards). The existing security rating (ESR) for an asset at any time *t*, would reflect these gradual changes. When an improvement is performed, the security rating should increase promptly which can be measured as a final security rating (FSR). For example, an improvement to rehabilitate a bridge would provide current design standards for the construction, thereby improving the bridge's physical structure and resilience. This change in security rating offers another measure of effectiveness for an improvement alternative.

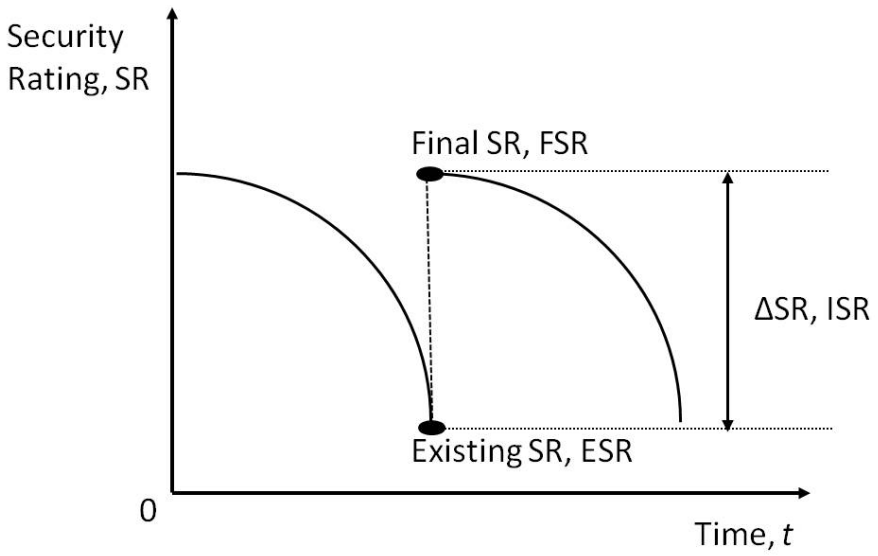


Figure 7.1. Conceptual Changes in Security Rating over Time

7.3. Using Security Rating in Prioritizing Transportation Security Investments Only

To incorporate the security rating into a multi-criteria evaluation as a performance measure, the ESR is used in order to capture the current state of an asset as a generic performance measure without the influence of an alternative (Table 7.1.). The increase in security rating (ISR) is an alternative-specific measure that captures the alternative's influence on the security of an asset (Table 7.2.). The FSR is another alternative-specific measure that provides an interaction measure between an asset's current security rating and the effects the improvement would cause (Table 7.3.). The ESR allows the decision-maker to prioritize assets based on their current security rating without the influence of improvement benefits. This evaluation is useful to determine which assets have the greatest need for security improvements at the current time. The ESR does not indicate the overall effects of an improvement to a transportation infrastructure network. This evaluation method should be used for asset-level prioritization. The ISR evaluation

method allows a decision-maker to determine the extent an improvement may influence the security of an asset. This method may be misleading if only alternatives with large security increases are considered. The alternatives with small security increases should not be ruled out solely due to this method. The FSR provides the decision-maker with the security rating of an asset after an improvement is completed. This method is useful to determine the overall security improvement to a transportation network. The drawback of this method is that greater consideration is given to assets that start with a high security rating where an improvement could only increase security further. Assets with lower security ratings increase in security but generally would not overcome those that started with large security ratings with this method. Each of these methods is useful in prioritizing security improvement alternatives based on the specific objective of interest to decision-makers.

Table 7.1. Simple Example of Existing Security Rating Prioritization

Asset	Existing Security Rating (ESR)	Priority Rank on the Basis of Existing Security Rating
Asset 1	3.22	3
Asset 2	2.45	1
Asset 3	5.65	4
Asset 4	7.40	5
Asset 5	8.18	6
Asset 6	3.12	2

The ESR prioritization indicates that assets with low initial security ratings should be placed at a higher priority level for improvements. In the example in Table 7.1., Asset 2 has the lowest security rating and would be given priority for further improvements.

Table 7.2. Simple Example of Increase in Security Rating Prioritization

Asset	Improvement	ESR[1]	ISR[1] (ΔSR)	Rank using ESR	Rank using ISR
Asset 1	Bridge Superstructure Reinforcement	3.22	4.57	3	2
Asset 2	Bridge Pier Improvement	2.45	3.00	1	4
Asset 3	Bridge Rehabilitation	5.65	4.00	4	3
Asset 4	Bridge Guardrail Replacement	7.40	0.52	5	6
Asset 5	Bridge Deck Repair	8.18	1.32	6	5
Asset 6	Bridge Substructure Reinforcement	3.12	4.88	2	1

[1]ESR: Existing Security Rating; ISR: Increase in Security Rating

The ISR prioritization indicates that the asset with the greatest associated improvement and, therefore, increase in security is given the highest priority. In the example in Table 7.2., Asset 6 would be given priority due to its relatively high increase in security. This example illustrates the drawback of only considering the increase in security, as opposed to focusing on the low ESR of Asset 2.

Table 7.3. Simple Example of Final Security Rating Prioritization

Asset	Improvement	ESR[1]	ISR[1] (ΔSR)	FSR[1] (SR + ΔSR)	Rank using ESR	Rank using ISR	Rank using FSR
Asset 1	Bridge Superstructure Reinforcement	3.22	4.57	7.79	3	2	5
Asset 2	Bridge Pier Improvement	2.45	3.00	5.45	1	4	6
Asset 3	Bridge Rehabilitation	5.65	4.00	9.65	4	3	1
Asset 4	Bridge Guardrail Replacement	7.40	0.52	7.92	5	6	4
Asset 5	Bridge Deck Repair	8.18	1.32	9.50	6	5	2
Asset 6	Bridge Substructure Reinforcement	3.12	4.88	8.00	2	1	3

[1]ESR: Existing Security Rating; ISR: Increase in Security Rating; FSR: Final Security Rating

The asset and alternative with the greatest security rating after an improvement is given the highest priority. In the example in Table 7.3., Asset 3 would be given highest priority. This example illustrates how this method could be misleading since the asset with the lowest ESR is prioritized last.

7.4. Using Security Rating in Evaluating Alternative Transportation Investments

The concept of security should be incorporated into multi-criteria evaluation by including security as one of the several performance measures already in use to evaluate transportation infrastructure investments. Traditionally, the performance measures used in project evaluation include:

- Air quality
- Noise
- Economic Efficiency
- Economic Development
- Travel Time
- Safety
- Vehicle Operating Costs (VOC)
- Connectivity

The prioritization of transportation assets typically utilizes performance measures related to asset characteristics, operations, and the surrounding environment. These criteria generally do not consider asset security, which is a function of the threat likelihood/magnitude, resilience of the transportation asset, and the resulting consequences of a potential threat. This implies that assets with low security do not receive the consideration they deserve during project evaluation and prioritization. It is feasible to add security as one of these criteria in transportation investment evaluation, prioritization, and decision making. The addition of a security performance

measure would increase the pool of available projects from which to select from when performing multi-criteria evaluation of alternative projects (Figure 7.2.).

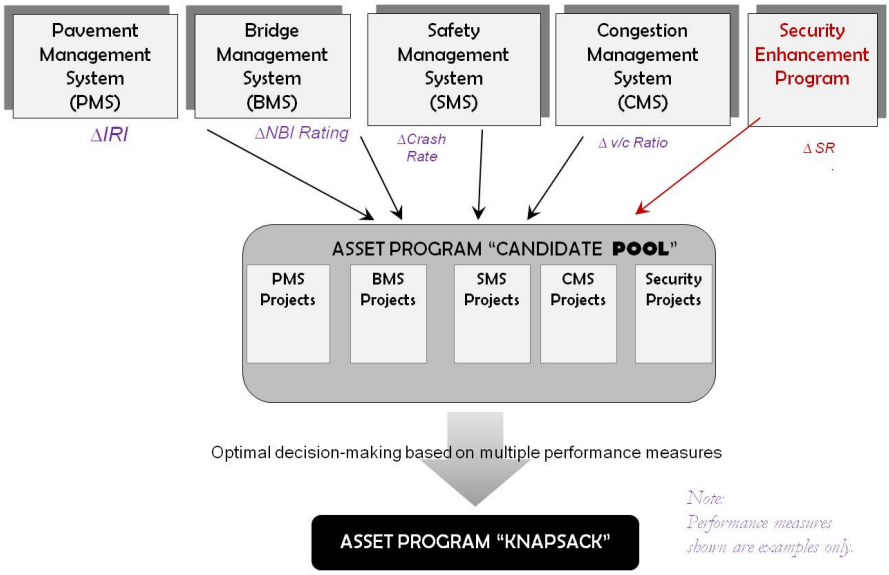


Figure 7.2. Multiple-Criteria Nature of Highway Investment Impacts

Secondly, the effectiveness of each alternative, regardless of type, can be converted into terms of security. The evaluation benefits can capture how well an improvement increases resilience and decreases potential consequences. Alternative evaluation is then performed based on the amount each alternative influences the security of an asset (Figure 7.3.). The security rating is useful to normalize the benefits of project alternatives, and should be considered a key performance measure in multi-criteria evaluation.

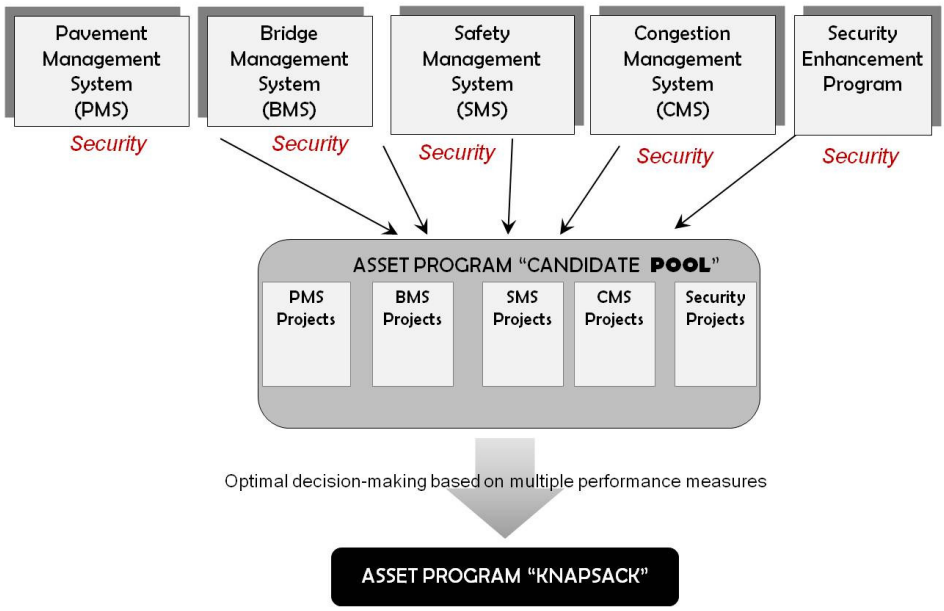


Figure 7.3. Importance of Security in Investment Evaluation

7.5. Chapter Summary

The evaluation of transportation assets typically utilizes performance measures related to asset characteristics, operations, and the surrounding environment. These evaluation methods generally do not consider asset security. This chapter provides a case for utilizing security as a performance measure by presenting example project alternatives prioritized by existing security ratings, increases in security ratings due to improvements, and the final security ratings after an improvement. The chapter further identified how security improvement projects should be included in a candidate project alternative pool and how each alternative in the pool can be prioritized based on their contribution to asset security. Security is a viable performance measure among the current performance measures identified for transportation project decision-making. The

next chapter provides a summary and discussion of the overall framework developed in this dissertation.

CHAPTER 8: CONCLUSION

8.1. Summary and Discussion

The first part of this dissertation provides an overview of the importance of transportation to society, the potential consequences that affect transportation services, current transportation security measures, and an overview of literature pertaining to different security methodologies. Many of the reviewed methods utilize a risk equation that identifies three main factors which, combined, provide a measure of risk. The first factor is the likelihood of threat, the second is the vulnerability of an asset due to a threat, and the third is consequences resulting should the asset become damaged or fail. Threat refers to any unexpected natural, unintentional man-made, or intentional man-made event that causes damage or disruption. Threat likelihood pertains to the probability of a threat occurring, either natural or man-made, that could cause the damage and/failure of the infrastructure being assessed. Consequence is defined as the collective costs and associated losses of damaged or destroyed infrastructure due to a threat. This dissertation provides an argument to retain the threat likelihood and consequence factors within the risk equation, while replacing the third factor with the concept of resilience. Resilience is a function of vulnerability, defined as the ability of infrastructure to resist and recover from a threat. Resilience captures the concept of vulnerability by accounting for the

weaknesses inherent in infrastructure that have the potential to fail. More specifically, in this dissertation, resilience is defined as the ability of infrastructure to withstand a potential threat.

The second part of the dissertation presents a framework for quantifying the security of transportation infrastructure based on three factors: threat likelihood, consequences of threats, and infrastructure resilience. The three factors are weighted and mathematically combined to provide a quantitative security rating for a transportation asset. Within each factor, a series of measures were identified in order to capture the performance of infrastructure in terms of resilience, threat likelihood, and potential consequences due to damage or failure. Furthermore, the measures are divided into attributes that incorporate a specific level of contribution, rated on a scale, to define the overall amount that each measure contributes to a specific security factor. The attributes are scaled so that they normalize distinct measurement units in order to be included into the security rating framework.

The John F. Kennedy Bridge in Jeffersonville, Indiana was identified as the asset-level case study to apply this security rating methodology. The security rating of the the John F. Kennedy Bridge was 1.31. This security rating, on a scale of zero to ten, is a relatively low rating and necessitates improvements. A network level case study was carried out for the bridge network in Indiana. The methodology determined that 2.34% of Indiana bridges have low security ratings (1.67<SR), 62.91% have low-to-medium security ratings (1.67<SR<5.0), 30.77% have medium-to-high security ratings (5.0<SR<8.35), and 3.99% of Indiana bridges have high security ratings (SR>8.35). Bridges in Indiana were grouped by material type, geographic region, roadway type, and

NHS status for further security analysis. The percentage of rural bridges with a security rating below 1.67 is 1.42%, while urban bridges have 4.12% below this rating. Interstate, U.S. route, and state route bridges had 0.55%, 2.42%, and 2.15% of their bridges below a security rating of 1.67 respectively. Non-NHS (National Highway System) bridges have 2.17% of their bridges below a security rating of 1.67, and NHS bridges have 2.64% of their bridges below this same rating. Steel, concrete, and pre-stressed concrete bridges had 3.73%, 0.69%, and 1.55% of their total bridges below the 0.4 security rating respectively. Additionally, bridges of concern could be spatially identified using ArcGIS and the security rating to determine areas of focus. Based on the network-level case study, the methodology would provide decision-makers with the ability to analyze transportation infrastructure at both the asset and network-level for security purposes.

In order to incorporate uncertainty, a fuzzy security rating was developed and a Monte Carlo simulation was run. A fuzzy security rating would allow for stochastic security factors to account for missing data or unknown measures. This method relies on expert opinion to determine the extent each factor affects overall security of an asset. In this case, each factor has a "high," "medium," or "low" level which determines the fuzzy security rating based on defined rules. As mentioned in Chapter 6, an example of a fuzzy rule is: If *resilience* is high, *consequence* is low, and *threat likelihood* is low then the *Security Rating* is high. Additionally, fuzzification of each measure and associated attributes can account for more uncertainty. A case study using the fuzzy security rating framework was performed for the Leo Frigo Memorial Bridge in Green Bay, Wisconsin. The fuzzy security rating of this bridge was 5.84, equating to a "medium" level of security. A Monte Carlo simulation was run to provide an average output for a bridge

given a probability distribution for each security factor. The mean sample security rating was 5.65, a medium rating indicating some improvements may be needed for security purposes.

Finally, a case was made to include security in multi-criteria evaluation. Prioritizing security investments and including security in the plethora of criteria for evaluation was explored. Decision-makers would be able to use the security rating framework to identify infrastructure in need of improvement based on the asset's current security rating, an increase in security rating due to a potential improvement, and a final security rating of an asset after an improvement was completed. Security as a performance measure for all project types would enable decisions to be made based on the alternative's contribution to asset security.

8.2. Future Improvements

This dissertation provides a framework for quantifying security in terms of asset resilience, threat likelihood, and consequences due to threats. The methodology it outlines has the potential to be utilized in fields outside of transportation in order to provide security ratings for varying types of infrastructure. In this case, new experts must be consulted to develop specific rating scales as well as to provide weights to each individual security measure and factor. The scales in this dissertation, however, are linear in nature and should be enhanced through non-linear models. Future work in this area would provide a security rating scale based on the new attribute scales and specifically identified measures of importance.

Optimization models already in practice should be run with the inclusion of the security rating performance measure, and any variations to the final output should be analyzed. Interaction effects between performance measures could be analyzed in a separate model. Conversion of project alternatives from various transportation improvement systems (e.g., pavement management system, safety management system, and congestion management system) should be measured in terms of security and input into the optimization model. This optimization model would be able to determine the benefits of making alternative decisions with the context of security.

8.3. Conclusion

The risk methodologies reviewed in the literature tend to provide differing definitions for similar security factors and combine these factors in a myriad of techniques. These methods rely on the current risk equation which relates the factors of threat likelihood, vulnerability, and consequence. The proposed security rating framework improves this equation by including the factor of resilience. Resilience is defined as the ability of infrastructure to withstand threats. With these three factors, a framework was developed to provide decision-makers with a method to quantify security for transportation infrastructure. The framework outlines the measures and attributes associated with each factor that contribute to security. The framework was fuzzified and a Monte Carlo simulation was run to account for uncertainty within the method. Threats are highly non-deterministic, therefore it is beneficial to include a probability distribution and range of factor levels in the framework. This helps to provide a range of potential security

outcomes. Finally, security should be considered as a performance measure within transportation project evaluation itself. Decision-makers would then gain the ability to prioritize infrastructure improvements based on their security contribution, by including security as one of the many performance measures in multi-criteria evaluation. Security of transportation infrastructure is integral to keep people and goods moving throughout the world. The transportation sector provides millions of employment opportunities and greatly contributes to the gross domestic economy of the United States. Without transportation, most activities would come to a standstill and lead to an immense economic decline. Protection of transportation infrastructure is of the utmost importance in order to maintain the quality of life needed for a country to run, and continue to run, efficiently.

LIST OF REFERENCES

AAR. (2012). Class I Railroad Statistics. Association of American Railroads. Accessed 5/10/12.

AASHTO. (2003). Recommendations for Bridge and Tunnel Security. American Association of State Highway and Transportation Officials. Transportation Security Task Force. Blue Ribbon Panel. Federal Highway Administration.

Ayyub, B.M. (2001). Elicitation of Expert Opinions for Uncertainty and Risks. CRC Press. New York.

Ayyub, B.M. (1992). Generalized Treatment of Uncertainties in Structural Engineering. Analysis and Management of Uncertainty: Theory and Applications. Elsevier Science Publisher B.V. pp. 235-246.

Ayyub, B.M. and Gupta, M.M. (1997). Uncertainty Analysis in Engineering and Sciences: Fuzzy Logic, Statistics, and Neural Network Approach. Kluwer Academic Publishers, Boston.

Ayyub, B. M., McGill, W. L., Kaminskiy, M. P. (2007). Critical Asset & Portfolio Risk Analysis: An All-Hazards Framework. Risk Analysis, Vol. 27, No. 4. pp. 789-801.

Barker, K., Ramirez-Marquez, J.E., Rocco, C.M. (2013). Resilience-based network component importance measures. Reliability Engineering & System Safety. Vol. 117. pp. 89-97.

BLS. (2011). Employment by Major Occupational Group. United States Department of Labor. Bureau of Labor Statistics. http://www.bls.gov/emp/ep_table_101.htm. Accessed 2/1/12.

BSI. (2011). Risk Management – Code of Practice and Guidance for the Implementation of BS ISO 31000. British Standards Institution.

Cambridge, J. and Parker, S. A. (2011). Security and Critical Infrastructure Protection: Progress and Paths to Resilience. TR News No. 275. July-August. Transportation Research Board.

Cellucci, T. A. (2010). Program Prioritization Index (PPI). Science and Technology, Commercialization Office. U. S. Department of Homeland Security.

Clark, E. and Philpott, D. (2011). CARVER+Shock Vulnerability Assessment Tool: A Six Step Approach to Conducting Security Vulnerability Assessments on Critical Infrastructure. Longboak Key, FL: Government Training Inc.

Clemen, R.T. (1989). Combining forecasts: A Review and Annotated Bibliography. International Journal of Forecasting, Vol. 5, pp. 559-583.

Clemen, R. T., and Reilly, T. (2001). Making Hard Decisions with DecisionTools®. Australia: South-Western CENGAGE Learning.

Coast Guard. (2003). Implementation of National Maritime Security Initiatives. Federal Register, Department of Homeland Security, Coast Guard. Vol. 68, No. 126, July 1, 2003, p. 39245.

DHSa. (2010). Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan. U.S. Department of Homeland Security.

DHS. (2010). Critical Infrastructure and Key Resources. US Department of Homeland Security, Washington, DC. http:/ //www.dhs.gov/files/ programs/gc_1189168948944.shtm. Accessed 4/22/10.

DHS. (2011). Critical Infrastructure Partnership Advisory Council. Department of Homeland Security.

Dojutrek, M. S., P A. Makwana, and S. Labi. (2012). A Methodology for Highway Asset Valuation in Indiana. Publication FHWA/IN/JTRP-2012/31. Joint Transportation Research Program, Purdue University, West Lafayette, IN.

Dojutrek, M.S., Volovski, M., Labi, S. (2014). Elemental Decomposition and Multi-Criteria Method for Valuing Transportation Infrastructure. Accepted for Publication in Transportation Research Record.

Dojutrek, M.S., Labi, S., Dietz, J.E. (2014). A Multi-criteria Methodology for Measuring the Resilience of Transportation Assets. Accepted for Publication in International Journal of Disaster Resilience in the Built Environment.

Dojutrek, M.S., Labi, S., Dietz, J.E. (2014). A Fuzzy Approach for Assessing Transportation Infrastructure Security. Proceedings of the 5th International Conference of Complex Systems Design and Management. November 2014, Paris, France. New York: Springer, 2014. Print.

EFC. (2006). Asset Management: A Guide for Water and Wastewater Systems. New Mexico Environmental Finance Center.

FDA. (2009). CARVER + Shock primer: An Overview of the CARVER plus Shock Method for Food Sector Vulnerability Assessments. U.S. Food and Drug Administration. http://www.fda.gov/Food/FoodDefense/FoodDefensePrograms/ucm376791.htm. Accessed April 14, 2014.

Federal Register. (2003). Maritime Vulnerability Self-Assessment Tool. Federal Register Vol. 68, No. 234, Doc. No. 03-30281. http://www.gpo.gov/fdsys/pkg/FR-2003-12-05/html/03-30281.htm.

FHWA. (2011). Freight Facts and Figures 2011: Miles of Infrastructure by Transportation Mode. http://ops.fhwa.dot.gov/freight/freight_analysis/nat_freight_stats/docs/11factsfigures/table3_1.htm. Accessed 1/6/12.

FHWA. (2012). Risk-based Transportation Asset Management: Evaluating Threats, Capitalizing on Opportunities. U.S. Department of Transportation, Federal Highway Administration.

FHWAa. (2014). Estimated U.S. Roadway Lane-Miles by Functional System. U.S. Department of Transportation, Federal Highway Administration. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_01_06.html. Accessed 11/22/14.

FHWAb. (2014). National Brisdge Inventory. http://www.fhwa.dot.gov/bridge/nbi.cfm. Accessed: 7/11/14.

Ferrell, W.R. (1985). Combining Individuals Judgments. Behavioral Decision Making, Plenum, NY.

Fisher, R. E., Norman, M. (2010). Developing Measurement Indices to Enhance Protection and Resilience of Critical Infrastructure and Key Resources. Journal of Business Continuity & Emergency Planning. Vol. 4, No. 3.

Flynn, S. (2000). Transportation Security: Agenda for the 21st Century. TR News 211, November-December 2000. Transportation Research Board. pp. 3-7.

Flynn, S. and Burke, S. (2011). Brittle Infrastructure, Community Resilience, and National Security. TR News No. 275. Transportation Research Board.

Ford, K.M. (2011). Incorporating Highway Asset Life Expectancy into Long-Term Fiscal Planning - A Risk-Based, Probabilistic Approach. Ph.D. Dissertation, Purdue University, School of Civil Engineering, West Lafayette, IN.

Frazier, E. R. (2009). Security 101: Primer on Protecting Agency Personnel and Assets. NCHRP Report 525, Vol. 14.

French, S. (1985). Group Consensus Probability Distributions: A Critical Survey, J.M. Bernardo et al. (Eds.), Bayesian Statistics, Elsevier, North Holland, pp. 183-201.

Garcia, M. L. (2001). Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann. Boston.

Gumus, A. T. (2009). Evaluation of Hazardous Waste Transportation Firms by using a Two Step Fuzzy-AHP and TOPSIS Methodology. Expert Systems with Applications. Vol 36. pp. 4067–4074. http://dx.doi.org/10.1016/j.eswa.2008.03.013.

Genest, C. and Zidek, J. (1986). Combining Probability Distributions: Critique and an Annotated Bibliography. Statistical Sciences Journal, Vol 1(1), pp. 114-148.

Haimes, Y. Y., Kaplan, S., Lambert, J. H. (2002). Risk filtering, ranking, and management framework using hierarchical holographic modeling. Risk Analysis, Vol. 22, Issue 2. pp. 381-395.

Henry, D., Ramirez-Marquez, J.E. (2012). Generic Metrics and Quantitative Approaches For System Resilience as A Function of Time. Reliability Engineering and System Safety, 99(1). pp. 114–22.

Herbst, B. (2012). Airline Industry-Year 2011. http://www.airlinefinancials.com/uploads/Airline_Industry_-_Year_2011_Review___Outlook.pdf. AirlineFinancials.com. Accessed 3/30/12.

Hooper, R., Armitage, R., Gallagher, A., Osorio, T. (2009). Whole-life Infrastructure Asset Management: Good Practice Guide for Civil Infrastructure. CIRIA. London.

IGS. (2014). IndianaMAP Data and Resources. Indiana Geological Survey. http://www.indianamap.org/index.php. Accessed: 11/14/13.

INGENIUM. (2006). International Infrastructure Management Manual. International Edition, Version 3.0, INGENIUM, Thames, New Zealand. www.nams.org.nz/International%20Infrastructure%20Management%20Mannual.

INCOSE (2012). Resilient Systems Working Group, www.incose.org.

Keeney, R. L., Raiffa, K. (1976). Decisions with Multiple Objectives: Preferences and Value Tradeoffs. Cambridge University Press, Cambridge, UK.

Kumar, I. Dojutrek, M., Labi, S. (2011). Assessing the Vulnerability of Indiana's Highway Bridges to Geo-Hazards. ASCE International Conference on Vulnerability and Risk Analysis and Management, April 2011, Hyattsville MD.

Labi, S. (2014). Introduction to Civil Engineering Systems. Wiley, Hoboken, NJ.

Labi, S., Bai, Q., Kumar, I., Ahmed, A., Anastasopoulos, P. (2011). Quantifying System Vulnerability as a Performance Measure for Systems Investment Evaluation and Decision-making. International Conference on Vulnerability and Risk Analysis and Management (ICVRAM) and ISUMA 2011 Fifth International Symposium on Uncertainty Modeling and Analysis. Hyattsville, MD.

Leung, M., Lambert, J.H., Mosenthal, A. (2004). A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks. Risk Analysis Journal, Vol. 24, No. 4. pp. 963-984.

MathWorks. (2013). MATLAB and Fuzzy Toolbox Release 2013a, The MathWorks, Inc., Natick, Massachusetts, United States.

McGill, W. L., Ayyub, B. M. (2007). Multicriteria Security System Performance Assessment Using Fuzzy Logic. Journal of Defense Modeling and Simulation Applications, Methodology, Technology. Vol. 4, No. 4. October. pp. 1-21.

McGill, W. L., Ayyub, B. M., Kaminskiy, M. P. (2007). Risk Analysis for Critical Asset Protection. Risk Analysis, Vol. 27, No. 5, pp. 1265-1281.

McGill, W. L. (2008). Critical Asset and Portfolio Risk Analysis for Homeland Security. Ph. D. Dissertation. University of Maryland. Department of Civil and Environmental Engineering. College Park, MD.

Melnick, E.L. and Everitt, B.S. (2008). Encyclopedia of Quantitative Risk Analysis and Assessment. John Wiley & Sons, West Sussex, England.

Moteff, J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Congressional Research Service. The Library of Congress.

Nachtmann, H., Pohl, E. A., Cassady, C. R., Kaya, O., Borin, S. (2007). Homeland Security for Rural Transportation Networks. Mack-Blackwell Rural Transportation Center. University of Arkansas.

NIICIE. (2007). CARVER2®: Critical Infrastructure Assessment Tool. National Infrastructure Institute Center for Infrastructure Expertise. Available at: http://wwww.ni2ciel.org/CARVER2.asp.

Palisade Co. (2014). Monte Carlo Simulation. http://blog.palisade.com/2008/12/29/monte-carlo-simulation-provides-advantages-in-six-sigma-v1/. Accessed 8/14/14.

PAS 55-2: 2008. Asset Management Part 2: Guidelines for the Application of PAS 55-1.

Patidar, V., La bi, S., Thompson, P.D., Sinha , K.C., (2008). Performance Measures for Enhanced Bridge Management. Transportation Research Record.

Phelps, N. (2013), "Leo Frigo closure costing about $139,000 per day in travel delay." http://www.greenbaypressgazette.com/article/20131109/GPG0101/311090331/. Accessed 11/25/13.

Philley,J. (2006). Collar Hazards with a Bow-Tie. Chemical Processing, Putman Media, January, pp. 27-34. http://www.nxtbook.com/nxtbooks/putman/cp016/index.php?startid=27. Accessed 4/22/10.

PHMSA. (2013). General Pipeline Facts. Pipeline and Hazardous Materials Safety Administration. U.S. Department of Transportation. http://phmsa.dot.gov/portal/site/PHMSA. Accessed 1/23/13.

Polzin, S.E. (2012). Security Consideration in Transportation Planning. STC White Paper. Center for Urban Transportation Research, University of South Florida. Accessed 10/12/12.

Porter, D. (2013), "Hurricane Sandy was second-costliest in U.S. history, report shows", available at: http://www.huffingtonpost.com/2013/02/12/hurricane-sandy-second-costliest_n_2669686.html. Accessed 10/12/13.

Ray, J. C. (2007). Risk-Based Prioritization of Terrorist Threat Mitigation Measures on Bridges. Journal of Bridge Engineering. ASCE. Vol 12. pp. 140-146.

Ridgwell, H. (2011), "Japan tsunami damage cost could top $300 billion", available at: http://www.voanews.com/content/japan-tsunami-estimated-costliest-ever-disaster-118644489/137021.html. Accessed 10/12/13.

Rodriguez, M. M., Labi, S., Li, Z. (2006). Enhanced Bridge Replacement Cost Models for Indiana's Bridge Management System. Transportation Research Record 1958. pp. 13-23.

SAIC. (2002). Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection. National Cooperative Highway Research Program Project 20-07/Task 151B.

SAIC. (2005). Reducing Security Risk for Transportation Management Centers. Presented at the 84th Annual Research Board Meeting, 2005.

SAIC & PB Consult. (2009). Costing Asset Protection: An All-Hazards Guide for Transportation Agencies (CAPTA). NCHRP Report 525, Vol. 15. Science Applications International Corporation & PB Consult. Transportation Research Board of the National Academies. Washington, D. C.

Secme, N. Y., Bayrakdarogly, A., Kahraman, C. (2009). Fuzzy Performance Evaluation in Turkish Banking Sector using Analytic Hierarch Process and TOPSIS. Esxpert Systems with Applications. Vol. 36. Pp. 11699-11709. http://dx.doi.gor/10.1016/i.eswa.2009.03.013.

Sinha, K. C., Labi, S. (2007). Transportation Decision Making Principals of Project Evaluation and Programming. John Wiley & Sons, Inc. New Jersey.

Smith, R.L., Bush, R.J., Schmoldt, D.L. (1997). The Selection of Bridge Materials Utilizing the Analytical Hierarchy Process. Proceedings of the ACSM/ASPRS Annual Convention and Exposition, Vol. 4, pp. 140-150.

Steffey, D. L. (2008). Homeland Security and Transportation Risk. Encyclopedia of Quantitative Risk Analysis and Assessment. England: John Wiley & Sons.

Sun, C. (2010). A Performance Evaluation Model by Integrating Fuzzy AHP and Fuzzy TOPSIS Methods. Expert Systems with Applications Vol. 37. pp. 7745–7754. http://dx.doi.org/10.1016/j.eswa.2010.04.066.

Tata, S. (2012), “60 freeway in Montebello to close for bridge demolition”, http://www.nbclosangeles.com/news/local/60-Freeway-Bridge-to-Close-For-Demolition-Montebello-Pomona-140664893.html (accessed 12 October 2013).

USDOT. (2012). Steel Bridge Design Handbook: Selecting the Right Bridge Type. Publication No. FHWA-IF-12-052-Vol.5.

USCG. (2010). MSRAM. Maritime Security Risk Analysis Model. Overview for USCG-CREATE Maritime Risk Symposium.

Venna, H. R., J. D., Fricker. (2009). Synthesis of Best Practices in Transportation Security, Volume I: Vulnerability Assessment. Joint Transportation Research Program, Indiana Department of Transportation and Purdue University, West Lafayette, IN.

Xia, J., Chen, M., Lie, R. (2004). A Framework for Risk Assessment of Highway Network. Presented at the 84th Annual Transportation Research Board Meeting.

Yang Z. L., Bonsall S., Fang, Q. G., Wang, J. (2007). Maritime Security-Assessment and Management. Journal of International Association of Maritime University. Vol. 5, Issue 1. pp. 56-72.

Yang, Z. L., Wang, J., Bonsall, S., Fang, Q. G. (2009). Use of Fuzzy Evidential Reasoning in Maritime Security Assessment. Risk Analysis. Vol. 29, No. 1, pp. 95-120.

Yazdani, M., Alidoosti, A., Basiri, M. H. (2012). Risk Analysis for Critical Infrastructures Using Fuzzy TOPSIS. Journal of Management Research, Vol. 4, No. 1, pp. 1-19.

Yue, Zh. (2011). An Extended TOPSIS for Determining Weights of Decision Makers with Interval Numbers. Knowledge-Based Systems,24: 146–153. http://dx.doi.org/10.1016/j.knosys.2010.07.014.